Популярные лекции
ПО МАТЕМАТИКЕ

Н. Н. ВОРОБЬЕВ

ПРИЗНАКИ ДЕЛИМОСТИ

АН
НИКИТИНА

ПОПУЛЯРНЫЕ ЛЕКЦИИ ПО МАТЕМАТИКЕ
ВЫПУСК 39

Н. Н. ВОРОБЬЕВ

ПРИЗНАКИ ДЕЛИМОСТИ

ИЗДАНИЕ ЧЕТВЕРТОЕ,
ИСПРАВЛЕННОЕ

МОСКВА «НАУКА»
ГЛАВНАЯ РЕДАКЦИЯ
ФИЗИКО-МАТЕМАТИЧЕСКОЙ ЛИТЕРАТУРЫ
1988

ББК 22.131
В75
УДК 511(023)

Воробьев Н. Н.

В75 Признаки делимости.— 4-е изд., испр.— М.: Наука. Гл. ред. физ.-мат. лит., 1988.— 96 с.— (Попул. лекции по мат.)

ISBN 5—02—013731—6

В брошюре систематически и с общей точки зрения описываются признаки делимости. Это дает автору повод популярно изложить некоторые вопросы элементарной теории чисел, теории отношений и теории алгорифмов.

3-е изд.— 1980 г.

Предназначается для учащихся старших классов средней школы.

В $\frac{1702030000-017}{053(02)-88}$ 53-88 ББК 22.131

ISBN 5—02—013731—6

© Издательство «Наука». Главная редакция физико-математической литературы, 1980, с изменениями, 1988

Светлой памяти
АНДРЕЯ АНДРЕЕВИЧА МАРКОВА,
создателя теории алгорифмов

ПРЕДИСЛОВИЕ

которое автор советует прочесть особенно внимательно

Современное школьное математическое образование ориентировано главным образом на воспитание у учащихся функционального мышления, на умение обращаться с непрерывными математическими объектами. Намечаемые изменения в школьных программах по математике идут в том же направлении. Вместе с тем в последнее время стали интенсивно разрабатываться новые области применения математики: составление программ для вычислительных машин, некоторые аспекты кибернетики и исследования операций, математическая экономика, математическая лингвистика и т. д. Освоение этих областей науки наряду с совершенствованием классического аппарата требует развития комбинаторной техники, анализа дискретного и создания новых плодотворных абстракций. Перечисленные стороны математики должны освещаться и в научно-популярной литературе.

* * *

С опушки леса в чащу ведет множество тропинок. Они извилисты, они сходятся, расходятся вновь и пересекаются одна с другой. На прогулке можно только заметить обилие этих тропинок, походить по некоторым из них и проследить их направление в глубь леса. Для серьезного изучения леса нужно идти по тропинкам, пока они вообще различимы среди сухой хвои и кустиков черники. Для того чтобы добыть дары леса, приходится вовсе покидать хоженые тропинки и продираться сквозь сплетения колючих ветвей и сучьев.

Настоящую брошюру можно рассматривать как описание одной из возможных прогулок по опушке современной математики. Изложение основных фактов, относящихся к признакам делимости, является в ней поводом затронуть некоторые довольно абстрактные вопросы дискретной математики. К числу таких вопросов относятся, прежде всего, утверждения элементарной теории чисел, группирующиеся вокруг основной теоремы арифметики и анализа канонического разложения натурального числа на простые множители. Далее, сама делимость чисел рассматривается как отношение на множестве целых чисел, т. е. как реализация довольно общего и абстрактного понятия. Наконец, признаки делимости трактуются здесь как алгорифмы, перерабатывающие каждое число в ответ, делится ли оно на данное число или не делится. Автор счел целесообразным среди признаков делимости особо выделить «признаки равноостаточности», перерабатывающие числа в остатки при их делении на данное число.

Для того чтобы оттенить разнообразные взаимосвязи между отдельными математическими фактами и возможности различных подходов к одному и тому же предмету, некоторые утверждения устанавливаются двумя различными путями.

* * *

Книжка рассчитана на школьников старших классов, интересующихся математикой и (если не считать нескольких упоминаний о формуле бинома) не предполагает никаких предварительных знаний, кроме умения производить несложные тождественные преобразования. Однако логическая структура материала довольно сложна, так что усвоение его во всех деталях может потребовать немало внимания и терпения.

Читателю можно порекомендовать следующий план изучения книжки.

При первом чтении можно ограничиться лишь основным текстом § 1—4 и не решать задач (за исключением задач № 31, 34, 36, 45, 47, 49, 50). Это даст общее, описательное знакомство с предметом. Так как большинство неискушенных в математике людей убеждены в изначальной справедливости тео-

ремы об однозначном разложении натурального числа на простые множители (считая ее, по-видимому, своего рода аксиомой), они могут понимать теоремы 9—13 как ее следствия.

При втором чтении нужно попытаться самостоятельно доказать все теоремы в том порядке, в каком они приведены. Чтобы читатель не поддавался слишком часто соблазну пользоваться готовыми доказательствами теорем, все эти доказательства отнесены в особый раздел. Исключение составляет доказательство теоремы 7, которое призвано служить камертоном, настраивающим читателя уже при первом чтении на должный уровень строгости.

При втором же чтении следует изучить § 5, а также решать задачи основного текста.

Наконец, при третьем чтении изучается текст, набранный мелким шрифтом, и относящиеся к нему задачи.

Читателю, желающему углубить свои познания в области теории чисел, следует обратиться к классическому курсу: Виноградов И. М. Основы теории чисел. — М.: Наука, 1981.

Изучение абстрактной теории отношений на множестве и дальнейших связанных с этим вопросов можно рекомендовать по книгам: Курош А. Г. Лекции по общей алгебре. — М.: Наука, 1973; Скорняков Л. А. Элементы общей алгебры. — М.: Наука, 1983 или Биркгоф Г. Теория решеток. — М.: Наука, 1984.

Наконец, более подробное и систематическое разъяснение понятия алгорифма содержится в книге: Трахтенброт Б. А. Алгоритмы и машинное решение задач. — М.: Физматгиз, 1960, а строгое изложение теории алгорифмов можно найти в основополагающей монографии: Марков А. А. Теория алгорифмов. — М.: Изд-во АН СССР, 1954. — (Тр. мат. ин-та АН СССР им. В. А. Стеклова. — Т. 42.) или же в книге: Марков А. А., Нагорный Н. М. Теория алгорифмов. — М.: Наука, 1984.

Второе издание отличается от первого лишь отдельными редакционными улучшениями. За некоторые из них автор благодарен проф. Греллю (ГДР).

Н. Н. Воробьев

ПРЕДИСЛОВИЕ К ТРЕТЬЕМУ ИЗДАНИЮ

В третьем издании по сравнению с предыдущими более обстоятельно разъяснена алгорифмическая сущность признаков равноостаточности и делимости, а также вводится рассмотрение таких признаков в произвольных системах счисления.

Вырица
1979 г.

Н. Н. Воробьев

ПРЕДИСЛОВИЕ К ЧЕТВЕРТОМУ ИЗДАНИЮ

Четвертое издание отличается от третьего отдельными мелкими исправлениями.

Вырица
1987 г.

Н. Н. Воробьев

§ 1. ДЕЛИМОСТЬ ЧИСЕЛ

1. Сумма, разность и произведение двух целых чисел — всегда целые числа. Этот факт иногда принято называть *замкнутостью* множества целых чисел по отношению к действиям сложения, вычитания и умножения.

По отношению же к действию деления множество всех целых чисел замкнутым не является: частное от деления одного целого числа на другое может, вообще говоря, и не быть целым.

Поэтому при изучении обстоятельств, связанных с делением целых чисел, одним из первых встает вопрос о выполнимости этого действия для данных двух чисел, т. е. о *делимости* этих чисел. При рассмотрении остальных арифметических действий над целыми числами подобный вопрос, очевидно, не возникает.

В дальнейшем мы будем считать известными основные свойства арифметических действий над целыми числами, а также простейшие свойства равенств и неравенств. Под «числом» всегда, если не оговорено противное, далее будет пониматься целое число.

Как обычно, целые неотрицательные числа: 0, 1, 2, ... будут называться *натуральными*. Говоря о всех натуральных числах, мы будем пользоваться термином *множество всех натуральных чисел*.

Определение. Число a *делится* на число b (или, что то же самое, число b *делит* число a), если существует такое число c, что $a = bc$.

Этот факт называется *делимостью* числа a на число b и обозначается как $a \vdots b$.

Подчеркнем, что запись $a \vdots b$ означает не какое-то действие, которое надлежит произвести над числами a и b, а некоторое утверждение, касающееся этих чисел. В зависимости от того, каковы числа a и

b, утверждение $a \vdots b$ может быть верным или неверным. Так, например, $4 \vdots 2$ верно, а $4 \vdots 3$ — нет.

Для выяснения того, является ли утверждение $a \vdots b$ верным или нет, т. е. для выяснения делимости числа a на число b, имеется довольно много разнообразных способов. Один из них состоит в непосредственном делении числа a на число b. Однако такое деление часто оказывается слишком долгим и утомительным занятием, и естественно появляется желание установить истинность интересующей нас делимости, не производя фактического деления. Не лишним представляется и такое соображение: пока нас интересует только факт делимости числа a на число b; если же мы выполним деление, то мы попутно узнаем еще и частное от этого деления и остаток от него (если деление нацело «не получилось»); все эти числа, однако, для нас никакой ценности не представляют, так как мы в данный момент интересуемся только тем, будет ли остаток от деления равен нулю или нет. Значит, есть основания предполагать, что, выполняя деление, мы какую-то (и, по-видимому, немалую) часть работы потратили на получение «отходов производства». Можно надеяться, что более прямые способы выяснения делимости, чем «грубое» деление, которые не дадут нам столь обильных отходов, будут экономнее и позволят установить факт делимости более коротким путем. Эти надежды в действительности оправдываются, и такие способы выяснения делимости существуют. Они называются *признаками делимости.*

Некоторые признаки делимости, несомненно, известны читателю. Целью этой книжки является рассмотрение различных признаков делимости, главным образом с принципиальной стороны.

Сущность всякого признака делимости на данное число b состоит в том, что при его помощи вопрос о делимости любого числа a на b сводится к вопросу о делимости на b некоторого числа, меньшего чем a. (Нетрудно видеть, что проверка делимости обычным делением также основана на этой идее.)

Таким образом, признак делимости является математическим объектом весьма распространенной, хотя и не бросающейся в глаза природы. Это не формула, не теорема, не определение, а некоторый процесс, совершенно такого же типа, что и процесс

умножения чисел «столбиком» или, скажем, процесс вычисления одного за другим членов арифметической прогрессии.

Понятие признака делимости будет уточнено в следующем параграфе.

2. В определении делимости чисел ничего не говорится о том, сколько различных значений может иметь частное от деления данного числа a на данное число b. Выясним здесь этот вопрос до конца, чтобы в дальнейшем к нему больше не возвращаться.

Пусть

$$a = bc \tag{1.1}$$

и вместе с тем

$$a = bc'.$$

Из этих равенств мы получаем

$$bc = bc',$$

или

$$b(c - c') = 0.$$

Если при этом $b \neq 0$, то $c - c' = 0$, т. е. $c = c'$. Если же $b = 0$, то, очевидно, и $a = 0$, а равенство (1.1) выполняется при любом c.

Таким образом, на нуль делится только нуль, а частное от такого деления неопределенно. Именно это и имеется в виду, когда говорят о невозможности «деления на нуль». Если же делитель отличен от нуля и делимость имеет место, то частное имеет одно, вполне определенное значение.

Говоря о делении, мы всегда будем предполагать делитель отличным от нуля.

Установим несколько простейших свойств делимости.

Теорема 1. $a \vdots a$.

Это свойство делимости называется ее *рефлексивностью* (или возвратностью).

Теорема 2. *Если* $a \vdots b$ *и* $b \vdots c$, *то* $a \vdots c$.

Это свойство делимости называется ее *транзитивностью* (или переходностью).

Теорема 3. *Если* $a \vdots b$ *и* $b \vdots a$, *то либо* $a = b$, *либо* $a = -b$ (*антисимметричность* делимости).

Теорема 4. *Если* $a \vdots b$ *и* $|b| > |a|$, *то* $a = 0$.

Следствие. *Если* $a \vdots b$ *и* $a \neq 0$, *то* $|a| \geqq |b|$.

Теорема 5. *Для того чтобы* $a \vdots b$, *необходимо и достаточно, чтобы* $|a| \vdots |b|$.

На основании этой теоремы в дальнейшем достаточно ограничиваться рассмотрением случая, когда делитель есть положительное число. Равным образом делимость произвольных целых чисел сводится к делимости неотрицательных чисел.

Теорема 6. *Если* $a_1 \vdots b$, $a_2 \vdots b$, ..., $a_n \vdots b$, *то*

$$(a_1 + a_2 + \ldots + a_n) \vdots b.$$

Следствие. *Если сумма двух чисел и одно из слагаемых делится на некоторое число* b, *то другое слагаемое также делится на* b.

Не следует считать все эти теоремы очевидными и не нуждающимися в каком-либо особом доказательстве. Дело здесь даже не в том, что в математике доказательству подлежит всякое утверждение, кроме аксиом и определений. Доказательства этих фактов (например, того, что всякое число делится на себя) принципиально необходимы, так как они не могут быть получены только из определения делимости, а нуждаются в использовании свойств самих чисел.

Разобраться в этом подробнее поможет нам следующий пример. Такого рода примеры часто называются *моделями*.

Очевидно, сумма, разность и произведение четных чисел всегда четны. Вместе с тем деление одного четного числа на другое не всегда выполнимо, а если и выполнимо, то частное не обязательно четно. Поэтому можно ввести понятие четной делимости четных чисел.

Определение. Четное число a *четно делится* на четное число b, если существует такое четное число c, что $a = bc$.

Очевидно, для четной делимости теорема 1 неверна, так как, например, не существует такого четного числа c, для которого $a = ac$.

К вопросам, связанным с четной делимостью четных чисел, мы еще будем несколько раз возвращаться. Пример четной делимости показывает, что можно строить различные теории делимости с различными свойствами, и теоремы, верные для одних таких теорий, могут оказаться неверными для других.

Задачи. Доказать следующие утверждения.

1. $0 \vdots a$.

2. $a \vdots 1$.

3. Если $1 \vdots a$, то $a = 1$.

4. Каково бы ни было $a \neq 0$, существует такое отличное от a число b, что $b \vdots a$.

5. Каково бы ни было число a, существует такое число b, что из $b \vdots c$ и $c \vdots a$ следует либо $c = b$, либо $c = a$.

6. Доказать теоремы, аналогичные теоремам 2, 3, 4 и 5, для четной делимости.

7. Построить такую теорию («модель») делимости, в которой теоремы 1, 3 и 4 были бы верными, а теоремы 2 и 6 — нет.

3. Уже при самом беглом знакомстве с конкретными фактами делимости бросается в глаза следующее обстоятельство: возможности делимости чисел практически не связаны с их величиной. С одной стороны, существуют маленькие числа, которые делятся на сравнительно большое количество чисел. Например, 12 делится на 1, 2, 3, 4, 6 и 12; число 60 имеет 12 делителей. Таким богатым делителями числам можно противопоставить весьма большие числа, которые имеют минимальное число делителей, т. е. 2 (согласно теореме 1 и задаче 2 каждое отличное от единицы число делится хотя бы на два различных числа). Хотя в действительности и известны некоторые закономерности, связывающие свойства делимости чисел с их величиной, но эти закономерности носят столь сложный и запутанный характер, что мы не будем их здесь касаться.

4. Тем более интересным оказывается тот факт, что сама делимость позволяет установить среди чисел некоторый порядок, отличающийся от их обычного порядка по величине, но имеющий с ним много общего.

В самом деле, вдумаемся, какой точный смысл вкладывается в слова о возможности упорядочить натуральные числа по их величине. Под этой возможностью, как нетрудно видеть, понимается то, что для некоторых пар чисел a и b имеет место отношение «больше или равно»:

$$a \geqq b,$$

которое означает, что разность $a - b$ неотрицательна (т. е. должно существовать такое натуральное число c, что $a = b + c$). Но ведь и явление делимости состоит в том, что отдельные пары чисел a и b подчиняются некоторому, вполне определенному условию (именно: существует такое целое c, что $a = bc$)! Таким образом, отношение делимости и отношение «больше или равно» представляют собой понятия

одной природы, и потому можно говорить об их общих свойствах или, наоборот, противопоставлять их друг другу.

В частности, подобно отношению делимости, отношение «больше или равно» между двумя натуральными числами является некоторым высказыванием об этих числах и может быть верным (например, $5 \geqq 3$) или неверным (например, $3 \geqq 5$).

Заметим сразу же, что отношение «больше или равно» имеет больше общих свойств с отношением делимости, чем отношение «больше». Это связано с тем, что отношение «больше или равно», подобно отношению делимости, рефлексивно (действительно, соотношение $a \geqq a$ справедливо для любого a), а отношение «больше» рефлексивным не является (неравенство $a > a$ не имеет места никогда). Именно поэтому здесь в качестве отношения порядка между натуральными числами рассматривается отношение «больше или равно», а не, казалось бы, более простое и естественное отношение «больше».

5. Отношение $\geqq$ обладает следующими легко проверяемыми свойствами:

1° $a \geqq a$ (рефлексивность).

2° Если $a \geqq b$ и $b \geqq a$, то $a = b$ (антисимметричность).

3° Если $a \geqq b$ и $b \geqq c$, то $a \geqq c$ (транзитивность).

4° Во всякой последовательности натуральных чисел

$$a_1 \geqq a_2 \geqq a_3 \geqq \ldots \geqq a_n \geqq \ldots,$$

все члены которой отличны друг от друга, найдется последнее число. Это свойство отношения иногда называется свойством *полной упорядоченности* множества натуральных чисел.

Свойство полной упорядоченности довольно сложно по формулировке и выглядит несколько искусственно. Однако оно вскрывает чрезвычайно важные черты в строении множества натуральных чисел, упорядоченных отношением $\geqq$. Из него выводятся многие другие свойства этого отношения. Кроме того, мы увидим, что именно на нем основаны столь употребительные в разных вопросах математики рассуждения «по индукции».

В качестве полезного применения этого свойства отметим следующее: существует такое число a, что из $a \geqq b$ следует $a = b$ (здесь a и b — натуральные числа).

В самом деле, если бы такого числа не было, то мы могли бы по каждому a_n находить такое a_{n+1}, что $a_q \geqq a_{n+1}$, но $a_n \not\geqq a_{n+1}$. Начав с произвольного a_1, мы получили бы последовательность

$$a_1 \geqq a_2 \geqq a_3 \geqq \ldots \geqq a_n \geqq a_{n+1} \geqq \ldots,$$

в которой все члены различны и которая никогда не кончается. Но существование такой последовательности противоречит свойству полной упорядоченности множества натуральных чисел.

Таким образом, указанное число a действительно существует. Оно называется *первым*, или *минимальным*, числом (очевидно, это нуль). Заметим здесь же, что мы сейчас не установили единственности минимального числа. Эта единственность будет зафиксирована далее специальным рассуждением.

5° Каково бы ни было число a, существует отличное от a число b, для которого $b \geqq a$.

Это свойство множества натуральных чисел называется его *неограниченностью* в смысле отношения $\geqq$.

6° Каково бы ни было число a, не являющееся минимальным, существует такое b, что $a \geqq b$, $a \neq b$ и для любого числа c из $a \geqq c \geqq b$ следует либо $c = a$, либо $c = b$. Это формальное утверждение в переводе на содержательный язык означает, что каждое натуральное число, кроме нуля, имеет непосредственно предшествующее натуральное число. (Иначе это можно сформулировать так: среди всех чисел, меньших данного, есть наибольшее.)

7° Либо $a \geqq b$, либо $b \geqq a$. Это свойство отношения называется его *дихотомичностью*, а также *полнотой*. В математике термин «дихотомичность» обычно выражает обязательную реализацию одной из двух возможностей. Само это слово греческого происхождения и означает «возможность разделения на две части».

Подчеркнем, что 1°—7° являются свойствами самого отношения на множестве всех натуральных чисел, а не свойствами тех или иных чисел, связываемых этим отношением. Поэтому вполне может оказаться, что для какого-нибудь другого отношения, связывающего числа в пары, но не по величине, а каким-либо иным способом, некоторые из утверждений 1°—7° могут оказаться и неверными.

Задача 8. Опираясь только на свойства 1°—7° отношения $\geqq$ и не пользуясь никакими свойствами самих чисел и действий над ними:

а) доказать единственность минимального числа;

б) доказать единственность непосредственно предшествующего числа;

в) сформулировать определение числа, непосредственно следующего за данным числом a (т. е. числа $a + 1$), и доказать его существование и единственность.

Задача 9. Проверить, какие из утверждений 1°—7° остаются в силе для отношения «больше» ($>$).

6. Справедливость свойств отношения $\geqq$ (как, впрочем, и любого другого отношения) может быть установлена двояко. Во-первых, мы можем воспользоваться свойствами тех или иных чисел или известными особенностями строения множества всех натуральных чисел. Именно так и проверялись нами свойства 1°—7°. Во-вторых, мы можем, уже убедившись в справделивости свойств 1°—7°, отвлечься от того, что отношение $\geqq$ связывает числа в пары, и выводить дальнейшие свойства этого отношения только из его свойств 1°—7°. Так нами были доказаны существование минимального числа и утверждения задачи 8.

Второй подход к вопросу весьма употребителен в современной математике и носит название *аксиоматического*. При таком подходе устанавливаются некоторые *аксиомы* (в нашем случае ими являются утверждения 1°—7°), которые отражают основные свойства изучаемых предметов и не подлежат доказательству, а из них чисто логическим путем, без повторного обращения к

свойствам исследуемых предметов, выводятся все остальные утверждения, которые называются *теоремами*.

Быть может, некоторым из читателей рассмотрение свойств отношений в отрыве от связываемых этими отношениями объектов (например, чисел) покажется тем верхом математической абстракции, который в практической жизни совершенно не нужен. По этому поводу следует сделать два замечания.

Во-первых, с точки зрения современной математики все приводимые здесь рассуждения вовсе не являются «особенно абстрактными». Более того, математикам уже давно приходится рассматривать одновременно много отношений и даже (!) связывать пары различных отношений новыми отношениями (так сказать, отношениями «второго порядка»).

Изложенный до сих пор материал позволяет проиллюстрировать примером понятие отношения между отношениями.

Пусть α, β, ... — некоторый набор отношений, связывающих натуральные числа. Это значит, что для любой пары чисел a и b и любого отношения γ из нашего набора мы знаем, связывается ли пара a, b отношением γ или нет. Если a и b отношением γ связаны, будем писать $a\gamma b$.

Будем говорить, что отношение α *сильнее* отношения β, и записывать это как $\alpha \supset \beta$, если любая пара чисел, связанная отношением β, оказывается, также связанной и отношением α, т. е. если из $a\beta b$ следует $a\alpha b$.

Так, например, обозначая отношение четной делимости через $\vdots_{\text{ч}}$, мы можем написать $\vdots \supset \vdots_{\text{ч}}$. Далее, очевидно, что $\geqq \supset >$, а также $\geqq \supset \vdots$. Вместе с тем существуют естественные отношения на множестве натуральных чисел, относительно которых нельзя утверждать, что одно из них сильнее или слабее другого. Так, например, если для двух натуральных чисел a и b полагать $a > b$, если последняя цифра в десятичной записи числа a больше последней цифры числа b, то не будет ни $> \supset \geqq$, ни $\geqq \supset >$.

Конечно, для свободного оперирования столь сложными понятиями, как отношения между отношениями, необходима специальная тренировка.

Во-вторых, такие и даже еще более отвлеченные рассуждения все чаще и чаще начинают встречаться в приложениях математики к экономике, биологии, лингвистике, военному делу. К сожалению, более подробные пояснения на этот счет увели бы нас слишком далеко от основного предмета.

7. С упорядоченностью множества натуральных чисел отношением $\geqq$ тесно связана возможность применять метод *полной индукции* (называемый также методом *совершенной* индукции или методом *математической* индукции). Обычно этот метод применяется в следующей форме. Пусть $A(n)$ — некоторое утверждение, касающееся произвольного натурального числа n. Это, по существу, означает, что мы имеем дело с бесконечной последовательностью утверждений

$$A(0),\ A(1),\ \ldots,\ A(n),\ \ldots,$$

каждое из которых относится к соответствующему натуральному числу. Предположим, что:

а) справедливо утверждение $A(0)$ («основание индукции»)*);

б) из справедливости утверждения $A(n)$ следует справедливость утверждения $A(n+1)$ («индуктивный переход»).

Принцип математической индукции утверждает, что в предположениях а) и б) $A(n)$ справедливо для любого натурального n.

Принцип математической индукции не является каким-то самостоятельным утверждением, а может быть выведен из свойств 1°—7° упорядочения множества натуральных чисел отношением $\geqq$.

Действительно, предположим, что условия а) и б) принципа индукции для утверждений $A(n)$ выполнены, но заключение этого принципа не имеет места. Последнее означает, что должны существовать такие числа m, для которых утверждение $A(m)$ неверно. Пусть m_1 — одно из таких чисел. Если для всех $n < m_1$ утверждение $A(n)$ верно, то m_1 — наименьшее из чисел, для которых $A(n)$ не имеет места. Если же $A(n)$ верно не для всех $n < m_1$, то должно существовать такое $m_2 < m_1$, что $A(m_2)$ неверно.

В итоге мы приходим к некоторой последовательности различных чисел

$$m_1 \geqq m_2 \geqq \ldots \geqq m_r \geqq, \ \ldots, \tag{1.2}$$

для каждого из которых $A(m)$ не имеет места. По свойству полной упорядоченности 4° в последовательности (1.2) должен быть последний член m_r. Очевидно, число m_r является наименьшим из всех чисел, для которых $A(n)$ неверно.

Поскольку $A(0)$ верно по условию, $m_r \neq 0$, так что существует число m_r^*, непосредственно предшествующее m_r (в действительности этим числом является $m_r - 1$). Так как $m_r^* < m_r$, утверждение $A(m_r^*)$ должно быть верным. Но тогда по условию б) принципа математической индукции должно быть верным также и утверждение $A(m_r^* + 1)$, т. е. $A(m_r)$, и мы получили противоречие. Это противоречие показывает, что нет чисел m, для которых $A(m)$ не имело бы места (т. е. не было бы справедливо).

Сделаем следующее замечание. Проведенные только что рассуждения не следует считать ни доказательством принципа индукции, ни его обоснованием. Они означают лишь возможность вывода одного математического утверждения (метода индукции) из других (из свойств отношения $\geqq$). Сами же эти свойства принимались нами в качестве аксиом и потому не доказывались, а лишь проверялись. Всякая попытка их математического доказа-

*) Часто за основание индукции принимают утверждение $A(1)$. Очевидно, это различие не является существенным. Важно лишь, что основание индукции касается первого из рассматриваемых нами чисел.

тельства неизбежно натолкнулась бы на необходимость введения в качестве аксиом каких-то новых условий.

В частности, всякая проверка свойства полной упорядоченности должна использовать те же индуктивные рассуждения (читатель может в этом убедиться сам).

Методу математической индукции в его различных вариантах посвящены книги: Соминский И. С. Метод математической индукции. — М.: Наука, 1974; Головина Л. И., Яглом И. М. Индукция в геометрии. — М.: Гостехиздат, 1956, содержащие большое количество примеров применения этого метода. На протяжении данной книги этот метод также будет часто применяться.

Задача 10. Пусть пары объектов произвольной природы (ими могут быть числа, точки, функции, теоремы и т. д.) связываются некоторым отношением $\leftarrow$, которое обладает свойствами, аналогичными свойствам 1°—7°. Доказать, что тогда эти объекты (элементы) можно перенумеровать (т. е. выписать их в некотором порядке) $A_1, A_2, A_3, \ldots$ так, что $A_i \leftarrow A_j$ тогда и только тогда, когда $i \geqq j$.

Сказанное, по существу, означает, что отношение, обладающее свойствами 1°—7°, упорядочивает множество в линейную цепочку элементов:

$$A_1 \rightarrow A_2 \rightarrow A_3 \rightarrow \ldots$$

8. Вернемся, однако, к отношению делимости. В случае положительных чисел теоремы 1, 2, 3 и задачи 3, 4 и 5 показывают, что в утверждениях 1°—6° мы можем заменить отношение $\geqq$ отношением $\vdots$. Что же касается утверждения 7°, то в применении к делимости оно гласит: «из двух чисел хотя бы одно делится на другое».

Но это неверно! Таким образом, отношение делимости обладает всеми свойствами отношения порядка, за исключением одного. В связи с этим отношение делимости упорядочивает натуральные числа не в виде линейной цепочки, а иным, более сложным образом (см. рисунок). Заметим, что числа, близкие по величине, могут оказаться довольно «далекими» друг от друга в смысле делимости. Наглядно демонстрируют это числа 4 и 5 или 7 и 8.

Попробуем от делимости целых положительных чисел перейти к делимости чисел натуральных, т. е. включим в рассмотрение нуль. Тогда схема на рисунке пополнится клеткой, лежащей выше всех остальных клеток схемы, ибо нуль делится на любое число и ни одно из чисел, отличных от нуля, на нуль не делится.

Читателю предоставляется самостоятельно переформулировать и проверить измененные для этого случая утверждения 1°—7°.

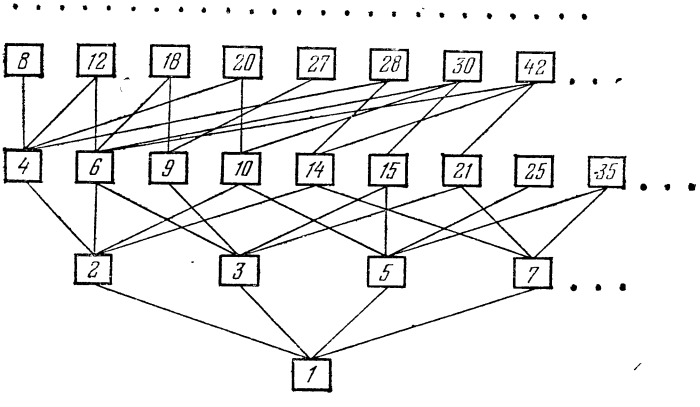
9. Определение. Любое отношение $\leftarrow$, подчиненное условиям:

1° рефлексивности ($a \leftarrow a$);

2° антисимметричности (из $a \leftarrow b$ и $b \leftarrow a$ следует $a = b$);

3° транзитивности (из $a \leftarrow b$ и $b \leftarrow c$ следует $a \leftarrow c$),

называется *частично упорядочивающим отношением.* Частично упорядочивающие отношения играют большую роль там, где «настоящее», линейное упорядочение не имеет места, например там, где каждый объект описывается или оценивается по нескольким различным, качественно несравнимым между собой показателям.



В качестве примера можно привести оценку результатов спортивных соревнований по нескольким различным видам спорта. Если одна из команд заняла по всем видам программы соревнований более высокие места, чем другая, то естественно считать, что первая команда добилась бо́льших успехов. Если же эти более высокие места были заняты по всем видам программы, за исключением, скажем, игры в крокет (которая почему-то на этот раз оказалась включенной в программу соревнований), где вторая команда оказалась сильней, то ответ на вопрос об окончательном распределении мест между нашими командами оказывается уже не столь очевидным. Энтузиасты игры в крокет могут даже настаивать на более высоком месте для второй команды. Во всяком случае любое суммарное распределение мест должно быть связано с некоторыми условными пересчетами (например, с приписыванием очков или «баллов»).

10. Условия 1°—3°, соблюдение которых делает отношение $\leqslant$ отношением частичного упорядочения, являются довольно свободными. Поэтому частично упорядоченными и притом упорядоченными весьма различными способами могут быть самые разнообразные объекты. В связи с этим о произвольном частично упорядочивающем отношении мало что можно сказать сверх того, что оно частично упорядочивающее. В частности, к объектам, для которых определено частично упорядочивающее отношение, нельзя, вообще говоря, применять метод математической индукции.

Дополним, однако, условия 1°—3° следующими:

4° полная упорядоченность;

5° неограниченность;

6° каждый объект, отличный от минимального, имеет непосредственно предшествующий;

8° каждый объект имеет не более конечного числа предшествующих;

9° каковы бы ни были a и $b \leftarrow a$ $(b \neq a)$, существует такое c, непосредственно предшествующее b, что $c \leftarrow a$.

Оказывается, что на основе частичной упорядоченности множества натуральных чисел отношением, которое удовлетворяет условиям 1°—6°, 8° и 9°, можно построить некоторое видоизменение метода индукции, состоящее в следующем.

Пусть снова $A(n)$ — утверждение, касающееся произвольного числа n. Предположим, что:

а) справедливо утверждение $A(a)$, где a есть минимальное число в смысле упорядочения $\leftarrow$;

б) если n — некоторое число и справедливость всех утверждений вида $A(m)$ для всех таких m, что $n \leftarrow m$ и $n \neq m$, установлена, то верно и утверждение $A(n)$.

Новая форма принципа индукции утверждает, что при соблюдении условий а) и б) утверждение $A(n)$ справедливо при любом n.

Задача 11. Вывести «новую форму» принципа индукции из ее «старой формы».

Так как отношение делимости условиям 1°—6°, 8° и 9° удовлетворяет (сформулируйте и проверьте для отношения делимости условия 8° и 9°), этот принцип индукции к отношению делимости применим.

В применении к делимости новый принцип индукции может быть сформулирован так: если некоторое утверждение $A(n)$ справедливо при $n = 1$ и из справедливости его для всех делителей числа n, отличных от n, следует его справедливость для n, то оно имеет место для любого числа.

11. Деление целых чисел, как мы уже говорили, выполнимо не всегда. Поэтому целесообразно наряду с действием деления рассматривать и другое, более общее действие, которое всегда выполнимо, а в случае выполнимости действия деления, по существу, совпадает с ним. Таким действием является *деление с остатком.*

Определение. *Разделить* число a на число b $(b > 0)$ *с остатком* — значит представить число a в виде

$$a = bq + r,$$

где $0 \leqq r < b$.

Число q при этом называется *неполным частным*, а число r — *остатком* от деления a на b. Очевидно, $r = 0$ тогда и только тогда, когда $a \vdots b$. В этом случае q равно частному от деления a на b.

Покажем, что деление с остатком всегда выполнимо, а неполное частное и остаток вполне определяются делимым и делителем, т. е. единственны.

Пусть сначала $a \geqq 0$. Будем выписывать одно за другим числа

$$a,\ a - b,\ a - 2b,\ \ldots \qquad (1.3)$$

до тех пор, пока не появится отрицательное число (очевидно, рано или поздно такое число должно появиться*)). Пусть последним из неотрицательных членов последовательности (1.3), т. е. самым маленьким из них, окажется число $a - bq$. Обозначая его через r, мы имеем

$$a = bq + r. \tag{1.4}$$

Очевидно, $r < b$ (иначе бы число $r - b$, т. е. $a - (q+1)b$, было бы неотрицательным, а этого не может быть, так как r — наименьшее из неотрицательных чисел среди (1.3)). Таким образом, (1.4) и является искомым представлением числа a.

Пусть теперь $a < 0$. Рассуждая аналогично предыдущему, будем выписывать последовательность чисел

$$a,\ a+b,\ a+2b,\ \ldots$$

до тех пор, пока не появится первое неотрицательное число r (легко проверить, что $r < b$). Пусть

$$r = a + bq'.$$

Тогда, обозначая $-q'$ через q, мы получаем

$$a = bq + r,$$

а это и требовалось.

Возможность деления с остатком доказана во всех случаях.

Докажем теперь однозначность этого деления, т. е. что из

$$a = bq + r \tag{1.5}$$

и

$$a = bq_1 + r_1 \tag{1.6}$$

следует

$$q = q_1, \quad r = r_1.$$

От такого доказательства единственности нельзя отмахнуться, попросту заявив, что, так как, дескать, действие вычитания однозначно, последовательность (1.3) может быть построена единственным способом; последний ее неотрицательный член также вполне

*) Точнее говоря, это следует из полной упорядоченности множества натуральных чисел отношением $\geqq$.

определен; пусть это будет наше r ... и т. д. Такое рассуждение еще не избавляет нас от возможности получить другие значения q и r каким-нибудь совершенно иным путем.

Сопоставляя отношения (1.5) и (1.6), мы видим, что

$$bq + r = bq_1 + r_1,$$

откуда

$$r - r_1 = b(q_1 - q),$$

т. е. $r - r_1$ делится на b. Но $|r - r_1| < b$, а по теореме 4 это возможно лишь при

$$r - r_1 = 0,$$

т. е. при $r = r_1$. Но тогда

$$b(q_1 - q) = 0,$$

и ввиду неравенства нулю числа b

$$q_1 - q = 0,$$

т. е. $q_1 = q$. Однозначность деления с остатком доказана. Таким образом, нами доказана следующая теорема.

Теорема 7 (о делении с остатком). *Для произвольных чисел a и b $(b > 0)$ существуют и единственны такие числа r и q, что*

$$a = bq + r,$$

причем $0 \leqq r < b$.

Заметим, что, в частности, при $b = 1$ должно быть $r = 0$, откуда $a = q$. Это соответствует утверждению задачи 2. Ясно вместе с тем, что если $b > 1$, то $a > q$.

Задача 12. Сформулировать и доказать теорему о делении с остатком для четной делимости.

12. Определение. Число p, не равное единице, называется *простым*, если оно делится только на себя и на единицу.

Простыми числами являются, например, числа 2, 3, 5, 7, 11, 13 и т. д.

Число, отличное от единицы и не являющееся простым, называется *составным*.

Теорема 8. *Простых чисел бесконечно много.*

Это утверждение следует понимать так, что для каждого простого числа найдется еще хотя бы одно простое число, большее его

Всякое число, делящее одновременно числа a и b, называется *общим делителем* этих чисел. Наибольший из общих делителей чисел a и b называется их *наибольшим общим делителем* и обозначается обычно через (a, b).

Если наибольший общий делитель чисел a и b равен единице, то эти числа называются *взаимно простыми.*

Иначе говоря, числа a и b называются взаимно простыми, если они одновременно не делятся ни на какое число кроме единицы.

Теорема 9. *Если a и p — натуральные числа, причем число p простое, то либо $a \vdots p$, либо числа a и p взаимно просты.*

Всякое число, делящееся одновременно на числа a и b, называется *общим кратным* этих чисел. Наименьшее положительное общее кратное a и b называется *наименьшим общим кратным* этих чисел.

Теорема 10. *Если M — общее кратное a и b, а m — их наименьшее общее кратное, то $M \vdots m$.*

Теорема 11. *Наименьшее общее кратное двух взаимно простых чисел равно их произведению.*

Следствие. *Для того чтобы число a делилось на взаимно простые числа b и c, необходимо и достаточно, чтобы оно делилось на их произведение.*

Теорема 12. *Если $ab \vdots c$, причем числа b и c взаимно простые, то $a \vdots c$.*

Теорема 13. *Если произведение нескольких сомножителей делится на простое число p, то хотя бы один из сомножителей делится на p.*

Следствие. *Если p — простое и $0 < k < p$, то число сочетаний*

$$C_p^k = \frac{1 \cdot 2 \cdot \ldots \cdot (p-1)\, p}{1 \cdot 2 \cdot \ldots \cdot (k-1)\, k \cdot 1 \cdot 2 \cdot \ldots \cdot (p-k-1)\,(p-k)}$$

делится на p.

Теорема 14 (основная теорема арифметики). *Всякое целое положительное число, кроме единицы, может быть представлено в виде произведения простых сомножителей и притом единственным способом* (произведения, отличающиеся только порядком сомножителей, различными не считаются).

Основная теорема арифметики указывает на принципиальную возможность разложения любого числа

на простые сомножители. Однако практическое осуществление такого разложения встречает большие трудности, которые современная математика иногда еще не может преодолеть. Разложение больших чисел на множители или установление их простоты в настоящее время осуществляется на основе применения электронных вычислительных машин. Так, лишь совсем недавно было обнаружено, что число $2^{19937}-1$ (в нем более шести тысяч цифр) является простым.

Пусть некоторое число a разложено в произведение простых сомножителей. Объединяя равные сомножители, мы получим формулу вида

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}, \tag{1.7}$$

где $p_1, p_2, \dots, p_r$ — различные простые числа, а α_1, $\alpha_2, \dots, \alpha_r$ — некоторые целые положительные числа. Произведение, стоящее в правой части формулы (1.7), называется *каноническим разложением* числа a.

Теорема 15. *Для того чтобы числа a и b были взаимно простыми, необходимо и достаточно, чтобы ни один из простых сомножителей, входящих в каноническое разложение числа a, не входил в каноническое разложение числа b.*

Теорема 16. *Пусть* (1.7) *— каноническое разложение числа a. Тогда для делимости $b \vdots a$ необходимо и достаточно, чтобы было*

$$b \vdots p_1^{\alpha_1},\ b \vdots p_2^{\alpha_2},\ \dots,\ b \vdots p_r^{\alpha_r}.$$

Из этой теоремы вытекает, что делимость на произвольное число равносильна одновременной делимости на некоторые степени простых чисел.

Задача 13. Оценить сверху наименьший простой делитель составного числа a.

Теорема 17. *Пусть*

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$$

— каноническое разложение числа a. Тогда для делимости $a \vdots b$ необходимо и достаточно, чтобы каноническое разложение b имело вид

$$b = p_1^{\beta_1} p_2^{\beta_2} \dots p_r^{\beta_r},$$

где

$$0 \leqq \beta_1 \leqq \alpha_1,$$
$$0 \leqq \beta_2 \leqq \alpha_2,$$
$$\cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot$$
$$0 \leqq \beta_r \leqq \alpha_r.$$

Весьма важным для целей данной книги оказывается следующий факт.

Теорема 18. *Пусть m и t — натуральные числа. Тогда m можно представить в виде такого произведения $m = m_1 m_2$, что $(m_1, t) = 1$ и найдется такое k, для которого $t^k \vdots m_2$.*

Этот факт имеет свои далеко идущие алгебраические аналогии, но мы их затрагивать не будем.

Задача 14. Указать способ построения по каноническим разложениям двух чисел канонических разложений наименьшего общего кратного этих чисел и их наибольшего общего делителя.

Задача 15. Обозначим через $\tau(a)$ число различных делителей числа a (включая единицу и само число a). Показать, что для числа a с каноническим разложением $p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}$

$$\tau(a) = (\alpha_1 + 1)(\alpha_2 + 1) \ldots (\alpha_r + 1).$$

Задача 16. Найти a, если известно, что $a \vdots 12$ и $\tau(a) = 14$.

Задача 17. Каноническое разложение числа a имеет вид $p_1^{\alpha_1} p_2^{\alpha_2}$, а $\tau(a^2) = 81$. Чему равно $\tau(a^3)$?

Задача 18. Чему равно a, если $a = 2\tau(a)$?

Задача 19. Доказать, что, каково бы ни было $K > 0$, найдется такое натуральное число k, что для всякого числа a, имеющего k простых сомножителей, будет

$$\frac{\tau(a^2)}{\tau(a)} > K.$$

Задача 20. Верны ли для четной делимости аналоги теорем 11—14?

§ 2. ДЕЛИМОСТЬ СУММ И ПРОИЗВЕДЕНИЙ

1. Во многих случаях при делении с остатком интересно найти именно остаток от деления числа a на число b, а величина неполного частного от деления не играет роли.

Пусть, например, мы хотим узнать, какой день недели будет 1 января 2000 г. (разумеется, если до того срока сохранится действующий в настоящее время календарь). Легко справиться по календарю, что 1 января 1988 г. — пятница. Двенадцать лет, разделяющие эти даты, состоят из $12 \cdot 365 + 3$ (последнее слагаемое — число високосных лет за это время), т. е. из 4383 дней. Эти дни составляют 626 целых недель и еще 1 день. По прошествии 626 целых недель снова наступит пятница, так что еще через 1 день, 1 января 2000 г., будет суббота. Очевидно, для решения поставленной нами сейчас перед собой задачи совершенно неважно знать, сколько именно целых недель пройдет за 12 лет, а интересно только число дней, прошедших сверх этих недель.

С задачами такого рода приходится иногда сталкиваться историкам, особенно востоковедам, при сопоставлении дат, указанных по разным календарям.

Казалось бы, для нахождения остатка от деления одного числа на другое проще всего произвести деление с остатком непосредственно. Однако практически выполнить такое деление нередко представляется весьма затруднительным, особенно если подлежащее исследованию делимое задано в виде некоторого сложного выражения вроде, скажем, $2^{1000} + 3^{1000}$. Вместе с тем львиная доля этой работы будет потрачена на нахождение неполного частного, которое нам само по себе не нужно. Необходимо поэтому попытаться выработать способ нахождения остатка

непосредственно, минуя вычисление неполного частного.

Продемонстрируем один из таких приемов на только что решавшейся нами задаче о дате 1 января 2000 г. Мы можем рассуждать следующим образом. Каждый простой (невисокосный) год состоит из 365 дней, что составляет 52 полные недели и еще один день. Високосный же год составляет столько же недель и два дня. Значит, весь срок от 1 января 1988 г. до 1 января 2000 г. состоит из некоторого (совершенно неважно, какого) числа полных недель плюс число дней, равное числу содержащихся в этом сроке лет, причем каждый високосный год считается за два. Это число дней равно $12+3=15$. Исключив из него 2 полных недели, получаем 1 день, который и следует отсчитывать от нашей пятницы. Оказывается, такая «замена года днем» есть проявление весьма общего приема, изучением которого мы займемся в п. 3.

2. Другой пример, когда целью деления с остатком является получение именно остатка, а неполное частное рассматривается лишь как исходный материал для дальнейших операций, дает нам запись чисел в той или иной *позиционной системе счисления*. Напомним, что число A называется записанным в (позиционной) системе счисления с основанием t, или, короче, в «t-ичной» системе счисления (где t — целое положительное число, большее единицы), если оно представлено в виде

$$A=a_nt^n+a_{n-1}t^{n-1}+\ldots+a_1t+a_0,$$

где

$$0\leqq a_i<t \quad \text{при} \quad i=0,\ 1,\ \ldots,\ n. \tag{2.1}$$

Числа $a_0,\ a_1,\ \ldots,\ a_n$ называются *t-ичными* цифрами числа A *).

При $t=10$ мы получаем *десятичную* систему счисления. Запись числа в этой системе настолько привычна для нас, что, говоря о числе, мы обычно только в этой форме его себе и представляем. В действительности, однако, если соображения привычности перестают играть роль, как это, например, имеет место при фиксации чисел в электронных вычислительных

*) Элементарное, но вместе с тем глубокое изложение вопросов, связанных с системами счисления, содержится в книге: Фомин С. В. Системы счисления. — М.: Наука, 1987.

машинах, более удобными могут оказаться и другие системы счисления (двоичная, восьмеричная и т. д.).

Так как мы в этой книжке не будем рассматривать непозиционных систем счисления (например, записей чисел «римскими» цифрами), мы далее указание на их позиционность будем, как правило, опускать.

Ясно, что из (2.1) следует

$$A = (a_n t^{n-1} + a_{n-1} t^{n-2} + \ldots + a_1) t + a_0,$$

т. е. последняя t-ичная цифра a_0 числа A является остатком от деления A на t с остатком. Неполное частное от такого деления стоит здесь в скобках. Разделив это неполное частное на t с остатком, мы получим

$$(a_n t^{n-2} + a_{n-1} t^{n-3} + \ldots + a_2) t + a_1.$$

Остатком оказывается предпоследняя t-ичная цифра числа A. Продолжая этот процесс повторного деления с остатком на t, мы будем последовательно получать все t-ичные цифры числа A, считая справа налево (т. е., от низших разрядов к высшим). Очевидно (а точнее — в силу полной упорядоченности множества натуральных чисел по величине), этот процесс последовательного деления с остатком должен рано или поздно оборваться. В результате мы получим все t-ичные цифры числа A, т. е. его запись в t-ичной системе счисления.

Так, в частности, осуществляется перевод чисел из одной системы счисления в другую. Например,

$$\begin{aligned} 10\,000 &= 6 \cdot 1\,666 + 4, \\ 1\,666 &= 6 \cdot 277 + 4, \\ 277 &= 6 \cdot 46 + 1, \\ 46 &= 6 \cdot 7 + 4, \\ 7 &= 6 \cdot 1 + 1, \\ 1 &= 6 \cdot 0 + 1. \end{aligned}$$

Поэтому 10 000 в шестеричной системе счисления записывается как 114 144.

Из теоремы 7 вытекает, что каждое число можно записать в любой системе счисления и притом единственным образом.

3. Определение. Назовем числа a и b *равноостаточными* при делении на m, если остатки от деления a и b на m равны.

Установим несколько свойств равноостаточных чисел.

Теорема 19. *Для того чтобы числа a и b были равноостаточными при делении на m, необходимо и достаточно, чтобы $(a-b) \vdots m$.*

Следствие. *Если числа a и b равноостаточны при делении на m и $m \vdots d$, то a и b равноостаточны при делении на d.*

Теорема 20. *Если при делении на m числа $a_1, a_2, \ldots, a_n$ соответственно равноостаточны числам $b_1, b_2, \ldots, b_n$, то равноостаточными будут суммы $a_1 + a_2 + \ldots + a_n$ и $b_1 + b_2 + \ldots + b_n$, а также произведения $a_1 a_2 \ldots a_n$ и $b_1 b_2 \ldots b_n$.*

Следствие. *Если при делении на m числа a и b равноостаточны, то такими же являются и степени a^n и b^n при любом натуральном n.*

Теорема 20 и ее следствие дают уже довольно богатые возможности для нахождения остатков от деления. Приведем несколько примеров.

Пример 1. Найти остаток от деления на 3 числа

$$A = 13^{16} - 2^{25} \cdot 5^{15}.$$

Очевидно, при делении на 3 число 13 равноостаточно с 1,2 равноостаточно с -1, а 5 тоже с -1. Значит, на основании доказанного число A при делении на 3 равноостаточно с числом $1^{16} - (-1)^{25}(-1)^{15} = 1 - 1 = 0$, т. е. искомый остаток равен нулю, и A делится на 3.

Пример 2. Найти остаток от деления того же числа A на 37.

Представим для этого A в следующем виде:

$$A = (13^2)^8 - (2^5)^5 \cdot (5^3)^5.$$

Так как $13^2 = 169$ при делении на 37 равноостаточно с -16, $2^5 = 32$ равноостаточно с -5, а $5^3 = 125$ — с $+14$, то все число A равноостаточно с

$$(-16)^8 - (-5)^5 (+14)^5$$

или, что то же самое, с

$$(16^2)^4 + 70^5.$$

Но 16^2, т. е. 256, равноостаточно с -3, а 70 — с -4. Значит, A равноостаточно с

$$(-3)^4 + (-4)^5$$

или, что то же самое, с

$$81 - (2^5)^2,$$

а потому — с

$$81 - (-5)^2 = 81 - 25 = 56.$$

Наконец, 56 при делении на 37 равноостаточно с 19, которое неотрицательно и меньше 37 и потому является искомым остатком.

Задача 21. Найти остаток от деления:

а) $A = (116 + 17^{17})^{21}$ на 8; б) $A = 14^{256}$ на 17.

Задача 22. Доказать, что при любом n:

а) $(n^3 + 11n) \vdots 6$;

б) $(4^n + 15n - 1) \vdots 9$;

в) $(10^{3n} - 1) \vdots 3^{n+2}$;

г) при любом a $\left(a^{2n+1} + (a-1)^{n+2}\right) \vdots (a^2 - a + 1)$;

д) при любом k $(n^k - 1) \vdots (n - 1)$;

е) при любом нечетном k $(n^k + 1) \vdots (n + 1)$.

4. Равноостаточные при делении на m числа a и b называются также *сравнимыми по модулю* m. Это обозначается так:

$$a \equiv b \pmod m,$$

а сама эта формула называется *сравнением*.

Сравнимость двух чисел по некоторому фиксированному модулю m или, что то же самое, их равноостаточность при делении на m, также является некоторым отношением, связывающим между собой целые числа.

Отметим несколько свойств отношения сравнимости по модулю.

1° Рефлексивность: $a \equiv a \pmod m$.

Действительно, $a - a = 0 \vdots m$.

2° Симметричность: если $a \equiv b \pmod m$, то $b \equiv a \pmod m$.

В самом деле, если $(a - b) \vdots m$, то (хотя бы по теореме 5) и $(b - a) \vdots m$.

3° Транзитивность: если $a \equiv b \pmod m$ и $b \equiv c \pmod m$, то $a \equiv c \pmod m$,

Для доказательства достаточно заметить, что из $(a - b) \vdots m$ и $(b - c) \vdots m$ по теореме 6 следует, что $(a - c) \vdots m$.

Если некоторое отношение (обозначим его через $\sim$) обладает свойствами рефлексивности, симметричности и транзитивности, то оно называется отношением *эквивалентности* (или *эквивалентным отношением*). Простейшим примером отношения эквивалентности на множестве чисел является отношение равенства.

Задача 23. Эквивалентное отношение $\sim$ на множестве чисел разбивает это множество на такие классы (называемые классами эквивалентности), что любые два числа из одного класса связаны отношением эквивалентности, а никакие два числа из разных классов этим отношением не связаны. (Доказать.)

В этой задаче речь идет об отношении эквивалентности, связывающем числа. Однако это несущественно, и утверждение задачи справедливо для эквивалентных отношений, связывающих объекты совершенно произвольной природы.

Так как отношение сравнимости по модулю m — отношение эквивалентности, оно также разбивает множество целых чисел на классы. Эти классы называют *классами вычетов* по модулю m.

4° Число классов вычетов по модулю m равно m.

В самом деле, два числа a и b принадлежат одному классу вычетов по модулю m тогда и только тогда, когда они при делении на m дают один и тот же остаток. Но остаток при делении на m может принимать ровно m значений: 0, 1, 2, ..., $m-1$. Следовательно, и число классов равно m.

Отметим одно чрезвычайно интересное обстоятельство, являющееся уточнением следствия теоремы 19.

Для того чтобы каждый класс вычетов по модую m_1 содержался в некотором классе вычетов по модулю m_2, необходимо и достаточно, чтобы было $m_1 \vdots m_2$.

Действительно, рассмотрим класс вычетов K_1 по модулю m_1, содержащий число 0. Очевидно, класс K_1 состоит из всех чисел, дающих при делении на m_1 в остатке 0, т. е. делящихся на m_1. В частности, он содержит число m_1. Класс вычетов по модулю m_2, содержащий K_1, также содержит 0 и потому состоит из всех чисел, делящихся на m_2. Так как в него входит число m_1, должно быть $m_1 \vdots m_2$. Этим доказана необходимость; достаточность же очевидна.

Таким образом, отношение делимости можно определить через соотношения между классами вычетов. Этот прием позволяет определять делимость для объектов гораздо более общей и сложной природы, чем натуральные числа. Последовательное развитие этих идей приводит к теории групп, важной отрасли современной алгебры, имеющей приложения в геометрии, в теоретической физике и в кристаллографии.

Продолжим перечисление свойств сравнимости чисел. Из теоремы 20 немедленно следуют:

5° Если $a \equiv b \pmod m$ и $c \equiv d \pmod m$, то

$$a + c \equiv b + d \pmod m.$$

Задача 24. Если на множестве целых чисел задано эквивалентное отношение $\sim$, разбивающее это множество на m классов и такое, что из $a \sim b$ и $c \sim d$ следует $a + c \sim b + d$, то отношение $\sim$ есть сравнимость по модулю m (т. е. $a \sim b$ тогда и только тогда, когда $a \equiv b \pmod m$).

Следствие. *Если* $a \equiv b \pmod m$, *то для любого целого* r $a + r \equiv b + r \pmod m$.

6° Если $a \equiv b \pmod m$ и $c \equiv d \pmod m$, то $ac \equiv bd \pmod m$.

Свойства 5° и 6° показывают, что сравнения подобно равенствам можно почленно складывать и перемножать.

Задача 25. Сформулировать и доказать правила сокращения сравнений.

Задача 26. Если число p простое и a не делится на p, то никакие два числа из a, $2a$, $3a$, ..., $(p-1)a$ не сравнимы друг с другом по модулю p. Поэтому при делении на p чисел a, $2a$, $3a$, ..., $(p-1)a$ получим по одному разу все остатки, кроме 0.

Задача 27 (теорема Вильсона). *Для того чтобы число* p *было простым, необходимо и достаточно, чтобы* $(p-1)! + 1 = 1 \cdot 2 \cdot \ldots \cdot (p-1) + 1$ *делилось на* p.

Задача 28. Сформулировать и доказать для равноостаточности теорему, аналогичную теореме 16.

§ 3. ПРИЗНАКИ РАВНООСТАТОЧНОСТИ И ПРИЗНАКИ ДЕЛИМОСТИ

1. Весьма общий способ нахождения остатка от деления произвольного, но фиксированного натурального числа a на данное натуральное число m заключается в следующем. Будем строить последовательность натуральных чисел

$$a = A_0,\ A_1,\ A_2,\ \ldots, \tag{3.1}$$

равноостаточных при делении на m. Способ построения этой последовательности выберем такой, чтобы после всякого ее члена, большего или равного m, следовал еще хотя бы один член. Тогда, очевидно, всякий член последовательности (3.1), меньший чем m (если, конечно, такой существует), будет равен остатку от деления a на m. Таким членом может быть, например, последний член последовательности (опять-таки, если такой имеется).

Одним из простейших примеров последовательности (3.1) может служить последовательность (1.3) из п. 11 § 1:

$$a,\ a - m,\ a - 2m,\ \ldots$$

В сущности, к построению последовательностей такого типа сводятся задачи нахождения остатков в примерах 1 и 2 из предыдущего параграфа.

Всякий способ построения последовательности (3.1), обладающей последним членом, назовем *признаком равноостаточности при делении на* m.

Из только что приведенного примера следует, что одним из признаков равноостаточности при делении на m является процесс последовательного вычитания числа m до получения первого числа, меньшего m.

2. Очевидно, для уверенности в безотказности работы признака равноостаточности при делении на m

необходимо, чтобы он удовлетворял следующим трем требованиям.

1. Признак равноостаточности должен быть применим к любому натуральному числу a. Иными словами, каково бы ни было число a, конструируемая по нему последовательность (3.1) действительно должна обладать указанным выше свойством: после каждого ее члена, не меньшего чем m, должен следовать еще хотя бы один член. Это свойство признака называется его *массовостью*.

2. Признак равноостаточности должен быть точно *определенным*, т. е. число a должно вполне определять все члены последовательности (3.1), не оставляя места какой-либо произвольности.

3. Наконец, мы должны иметь гарантию того, что в последовательности (3.1) хотя бы один член будет меньше чем m. Это требование будет выполнено, если строить последовательность (3.1) так, чтобы она обязательно имела лишь конечное число членов, т. е. чтобы процесс ее построения не мог продолжаться неопределенно долго, а рано или поздно заканчивался появлением остатка от деления a на m. Сформулированное свойство признака равноостаточности называется его *результативностью*.

3. Процессы, обладающие свойствами массовости, определенности и результативности, называются *алгорифмами* и играют в современной математике важную и все более возрастающую роль.

Разумеется, только что приведенная характеризация алгорифма как процесса, обладающего тремя перечисленными свойствами, не является его точным определением. Такое определение, хотя и выработано современной математикой, но сравнительно сложно и не может быть здесь сформулировано. Однако перечисленные предъявляемые к алгорифмам требования довольно полно отражают те условия, которым должны удовлетворять называемые алгорифмами математические процессы. Роль алгорифмов определяется тем, что они являются единообразными способами решения целого ряда однотипных задач. Так, каждый признак равноостаточности позволяет находить остатки от деления варьируемого числа a на некоторое фиксированное m.

Говоря несколько вольно, к алгорифмам сводятся все те математические задачи, решение которых мож-

но автоматизировать. Поэтому не случайно развитие теории алгорифмов исторически совпало с появлением и распространением электронных вычислительных машин.

К алгорифмам сводятся не только вычислительные задачи в узком смысле этого слова, т. е. такие задачи, в которых по более или менее сложным правилам можно на основе исходных данных получить численный ответ. Можно также ставить вопрос о поисках алгорифма, позволяющего решать *любую* задачу из некоторой (разумеется, строго очерченной) области математики. Этот алгорифм должен уметь перерабатывать формулировки теорем в их доказательства. Как ни фантастично это может показаться, такие алгорифмы существуют, хотя и не для очень широких областей математики. Вместе с тем для некоторых ее областей (например, для любой области, охватывающей всю арифметику) таких алгорифмов принципиально быть не может.

4. Уточним применительно к признакам равноостаточности содержание, а также последствия от соблюдения трех предъявляемых к алгорифмам требований.

Из *массовости* признака равноостаточности вытекает, что он должен перерабатывать различные числа, и результаты этой переработки также должны быть, вообще говоря, различными (ибо при делении на какое бы то ни было $m > 1$ не все числа равноостаточны друг другу). Значит, необходимой составной частью этого процесса должно быть различение чисел (по их величине).

Свойство *определенности* признака равноостаточности означает, что уже выписанные числа $A_0, A_1, \ldots, A_n$ последовательности (3.1) должны быть настолько «опознаваемыми», чтобы на их основании можно было написать следующее число последовательности, A_{n+1}.

Наконец, свойство *результативности* влечет, кроме всего прочего, еще и необходимость неограниченных возможностей сравнивать (по величине) получаемое на каждом шаге нашего процесса число A_k с делителем m.

Таким образом, соблюдение каждого из трех требований алгорифмичности для признака равноостаточности упирается, прежде всего, в необходимость уметь сравнивать в произвольных парах числа по их

величине и указывать, если они различны, какое из них больше, а какое — меньше.

5. Только что упомянутая «необходимость уметь», очевидно, также имеет алгорифмическую природу: сравнению по величине должны подлежать любые два натуральных числа (массовость), результатом сравнения может быть не более чем один ответ: больше, меньше или равно (определенность), и этот ответ должен всегда достигаться (результативность). Значит, мы получаем основание говорить об алгорифмах сравнения двух чисел по величине. Построение такого алгорифма не является столь уж самоочевидным делом, как это могло бы показаться на первый взгляд. Например, вопрос о том, одинаковы или различны числа

$$2^{20} - 3 \cdot 5^2 \cdot 11 \cdot 31 \cdot 41 \quad \text{и} \quad 3^{10} - 2 \cdot 3 \cdot 13 \cdot 757, \tag{3.2}$$

и если различны, то какое из них больше, требует для своего решения известных усилий, хотя в действительности первое из этих чисел есть всего-навсего 1, а второе 3.

Ясно, что сравнение по величине чисел из (3.2) затрудняется формой их записи. Следовательно, для построения признаков равноостаточности весьма важно иметь дело с представлением чисел в такой форме, которая обеспечивала бы возможность их сравнения по величине. Такие формы записи существуют.

Например, ими являются записи чисел в тех или иных (позиционных) системах счисления (см. § 2, п. 2). Алгорифм сравнения двух чисел, записанных в одной и той же системе счисления, состоит в следующем.

1. Сначала в каждом из чисел зачеркиваются цифры по одной (начиная, скажем, справа); если после того, как одно из чисел окажется зачеркнутым полностью, в другом еще останутся цифры, то второе число будет больше первого; если же запасы цифр в обоих числах будут исчерпаны одновременно, то для сравнения чисел выполняется следующая процедура.

2. Записи сравниваемых чисел восстанавливаются, сравниваются их первые (слева) цифры. При этом большей цифре будет соответствовать большее число; если первые цифры оказываются одинаковыми, то сравниваются вторые цифры и т. д. до первого

различия цифр. При этом опять-таки бо́льшая цифра будет указывать на бо́льшее число. Если все соответственные цифры чисел окажутся одинаковыми, то числа будут равны.

При проведении второй из указанных процедур предполагается, что сравнение по величине однозначных, т. е. меньших чем основание системы счисления, чисел мы производить умеем. Это значит, что в каждой системе счисления исходные значки-цифры заранее задаются в некотором фиксированном порядке; например, в общепринятой десятичной нумерации значок «2» предшествует значку «3» в том смысле, что значок «2» описывает меньшее количество, чем значок «3».

С точки зрения такого алгорифмического сравнения чисел по величине все системы счисления теоретически равноценны. Сравнение же в этом смысле систем счисления по их практическому удобству может служить примером неалгорифмической постановки вопроса (не выполняется условие определенности), и мы на нем останавливаться не будем. Обратим только внимание на то, что в этом вопросе сила привычки к десятичной системе счисления никаких особых преимуществ этой системе не дает.

6. Кроме алгорифмов сравнения чисел, записанных в одной и той же системе счисления, существуют и алгорифмы выполнения арифметических действий над ними. Ими являются общеизвестные (и, очевидно, зависящие лишь несущественным образом от основания системы счисления) способы сложения, вычитания и умножения чисел «столбиком» и их деления «углом». Ясно, что в последнем случае было бы, пожалуй, уместнее говорить не просто о делении, а о делении с остатком.

В случае выполнения действий навыки в обращении с десятичной системой счисления приносят существенное облегчение. Например, выполнение в пятеричной системе счисления действия

$$\begin{array}{r|l} 13110 & 224 \\ \cline{2-2} 1232 & 31 \\ \cline{1-1} 240 & \\ 224 & \\ \cline{1-1} 11 & \end{array}$$

требует известных умственных усилий.

Из алгорифмичности деления с остатком, согласно сказанному в п. 2 § 2, вытекает и алгорифмичность перевода записей чисел из одной системы счисления в другую. Следовательно, можно говорить также об алгорифмах сравнения чисел и действий над ними, если они записаны в различных системах счисления. Как дальнейшее следствие отсюда получается, что алгорифмами являются всевозможные вычисления по арифметическим формулам, в которые вместо букв можно подставлять те или иные числа.

Обратим, наконец, внимание на то, что мы не говорим здесь об алгорифме самого процесса записи произвольно заданных натуральных чисел в той или иной системе счисления, ибо мало ли каким может оказаться это исходное задание.

7. В качестве иллюстративного примера рассмотрим следующее построение. Для каждого натурального числа n составим последовательность $a_0^{(n)}, a_1^{(n)}, a_2^{(n)}, \ldots$ однозначных чисел, являющихся цифрами бесконечного десятичного разложения числа $\sqrt{n}$ (если число n не является точным квадратом, то эта последовательность, очевидно, оказывается непериодической), и пусть $r_1^{(n)}, r_2^{(n)}, \ldots$ — номера всех тех цифр, которые равны нулю: $a_{r_i^{(n)}}^{(n)} = 0$ ($i = 1, 2, \ldots$). Если теперь число равных нулю цифр конечно (пусть последняя из них имеет номер $r_k^{(n)}$, так что $a_i^{(n)} > 0$ при $i > r_k^{(n)}$), то положим

$$f(n) = 10^{r_1^{(n)}} + 10^{r_2^{(n)}} + \ldots + 10^{r_k^{(n)}} + 1,$$

а если их число бесконечно, то положим, скажем, $f(n) = 0$. Каждое из чисел $f(n)$ является натуральным. Однако едва ли можно говорить об алгорифме, который перерабатывал бы число n в запись числа $f(n)$ в десятичной системе счисления.

Разумеется, вся неалгорифмичность этой конструкции состоит в требовании распознавать, будет ли в десятичном разложении $\sqrt{n}$ конечное или бесконечное число нулей. Между прочим, в известном смысле (в каком именно — мы не станем здесь выяснять) е с т е с т в е н н о в е р и т ь, что $f(n) = 0$ для любого натурального n.

8. Одним из наиболее важных в математике алгорифмов является так называемый *алгорифм Евклида*, который состоит в следующем.

Пусть a и b — два натуральных числа, причем $b > 0$. Разделим a на b с остатком: $a = bq_0 + r_1$, где $0 \leqq r_1 < b$. Если $r_1 \neq 0$, то мы имеем возможность разделить с остатком b на r_1: $b = r_1 q_1 + r_2$, причем $0 \leqq r_2 < r_1$. Продолжая эти последовательные деления с остатком на остаток от предыдущего деления, мы получим дальнейшие равенства: $r_1 = r_2 q_3 + r_3$, $r_2 = r_3 q_4 + r_4$ и т. д.

Покажем, что описанный процесс действительно является алгорифмом, т. е. обладает свойствами определенности, массовости и результативности.

Заметим, что рассматриваемый нами процесс состоит в последовательном выполнении действия деления с остатком.

Поэтому определенность и массовость этого процесса являются следствием неограниченной выполнимости и однозначности действия деления с остатком. Результативность нашего процесса устанавливается также довольно просто. Число b и остатки от делений, составляющих наш процесс, образуют, очевидно, убывающую последовательность неотрицательных чисел:

$$b,\ r_1,\ r_2,\ \ldots \tag{3.3}$$

Но число всех неотрицательных и не превосходящих b чисел равно $b + 1$. Поэтому и последовательность (3.3) не может насчитывать более чем b членов, так что наш процесс может состоять не более чем из b делений с остатком*). Таким образом, рассматриваемый процесс действительно является алгорифмом и вполне оправдывает свое название.

Выясним условия окончания процесса. Очевидно, последнее деление должно быть таким, чтобы дальнейшее деление на его остаток было уже невозможно. Но это может быть лишь в том случае, когда этот последний остаток равен нулю, т. е. когда последнее деление совершилось нацело.

Задача 29. а) Последний отличный от нуля остаток r_n в применении алгорифма Евклида к числам a и b есть (a, b).

б) Каковы бы ни были натуральные a и b, существуют такие целые A и B, что $aA + bB = (a, b)$.

Задача 30. Вывести из результата б) задачи 29 теоремы 9, 12, 13 и 14. (Подчеркнем, что наши рассуждения, связанные с алгорифмом Евклида, были основаны только на возможности деления с остатком. Мы не пользовались в них ни теоремами 9—14, ни какими-либо иными соображениями, опирающимися на основную теорему арифметики.)

9. Применение алгорифмов (их, так сказать, «работа») может оказаться достаточно громоздким. В качестве примера рассмотрим процесс получения по числу n его канонического разложения (иными словами, алгорифм, перерабатывающий натуральное число в его каноническое разложение). Для оттенения алгорифмической сущности этого процесса включим его как этап в процесс последовательного нахождения канонических разложений одного за другим всех натуральных чисел. Это дает нам основание вести рассуждения «по индукции» (см. п. 7 § 1). Предполо-

---

*) На самом деле число этих делений не может превосходить числа $5 \log_2 b$. Это следует из рассмотрения чисел Фибоначчи (см., например, книгу: Воробьев Н. Н. Числа Фибоначчи. — М.: Наука, 1984. — С. 82—83).

жим, что для всех чисел, меньших n, канонические разложения уже выписаны. Из этого списка можно (вполне алгорифмично) усмотреть, какие из чисел, меньших n, являются простыми. Перечислив их все по возрастанию, будем делить n на каждое из них (ввиду результата задачи 13 нам достаточно произвести деление лишь на те p, для которых $p^2 < n$). Если n разделится на некоторое p, то будет $n = n_1 p$ и $n_1 < n$, а каноническое разложение n_1 в нашем перечне по предположенному уже имеется. Поэтому каноническое разложение n получится из канонического разложения n_1 путем увеличения в нем показателя p на единицу.

10. Вернемся, однако, к признакам равноостаточности. Алгорифмическое построение последовательности (3.1) может быть осуществлено весьма разнообразными путями. Наиболее естественный из них состоит в следующем.

Попробуем найти функцию $f(x)$, подчиненную следующим условиям:

а) значение $f(x)$ при $x \geqq m$ есть натуральное число;

б) значение $f(x)$ при $x < m$ не определено (т. е. не имеет смысла);

(нет ничего удивительного в том, что та или иная функция теряет смысл при некоторых значениях аргумента; например, не имеет смысла значение функции $\frac{1}{x(x-1)}$ при $x = 0$ или при $x = 1$);

в) если $x \geqq m$, то $f(x) < x$;

г) если $x \geqq m$, то числа x и $f(x)$ равноостаточны при делении на m.

Такие функции существуют. Примером является функция $f_0(x)$:

$$f_0(x) = \begin{cases} x - m, & \text{если } x \geqq m, \\ \text{не определено}, & \text{если } x < m. \end{cases}$$

Именно эта функция и осуществляет построение последовательности (1.3) в п. 11 § 1.

Каждой функции $f(x)$, удовлетворяющей условиям а)—г), отвечает некоторый способ построения последовательности (3.1), т. е. некоторый признак равноостаточности при делении на m.

В самом деле, возьмем произвольное натуральное число a и будем строить последовательность чисел

$$A_0,\ A_1,\ A_2,\ \ldots, \tag{3.4}$$

где

$$A_0 = a \quad \text{и} \quad A_{k+1} = f(A_k) \quad \text{при} \quad k = 0,\ 1,\ \ldots \tag{3.5}$$

Если $A_k \geqq m$, то значение функции $f(A_k)$ определено, и потому за A_k следует хотя бы один член. Если же $A_k < m$, то $f(A_k)$ не определено, и A_k является последним членом последовательности (3.4).

Итак, мы действительно имеем некоторый признак равноостаточности.

11. Покажем, что найденный признак равноостаточности обладает всеми тремя свойствами алгорифма.

Условие массовости здесь соблюдается потому, что любое число дает начало некоторой последовательности (3.4), обладающей свойством (3.5).

Условие определенности соблюдается ввиду того, что для вычисления значений $f(x)$ функции f достаточно уметь сравнивать по величине числа x и m и выполнять операцию вычитания (отнимания m от x). Обе эти процедуры (если мы имеем дело с числами, записанными в некоторой системе счисления), как было выяснено, являются алгорифмами и тем самым обладают свойством определенности.

Обратимся к условию результативности. По самому своему построению функция f выбрана так, что члены последовательности (3.4) положительны и убывают. Поэтому в ней найдется наименьший неотрицательный член. (Номер этого члена, как нетрудно проверить, не превосходит числа a.) Если бы этот член (обозначим его через α) был больше или хотя бы равен m, то существовало бы значение $f(\alpha)$, по-прежнему неотрицательное, но меньшее α. Значит, член α не был бы последним среди неотрицательных членов последовательности (3.4). Следовательно, последний неотрицательный член (3.4) должен быть меньше чем m. Но тогда значение $f(\alpha)$ не имеет смысла, и α оказывается вообще последним членом нашей последовательности. Процесс построения последовательности, таким образом, заканчивается, и последний ее член является остатком от деления a на m.

В результате мы установили, что описанный нами признак равноостаточности действительно обладает требуемыми свойствами определенности, массовости и результативности, т. е. является алгорифмом.

12. Пользуясь изложенным в п. 9 приемом построения признаков равноостаточности, найдем несколько таких признаков. В соответствии со сказанным выше будем считать, что числа, остатки от деления которых требуется найти, записаны в позиционной системе счисления с некоторым основанием t. Признак равноостаточности при делении на некоторое m перерабатывает в остаток от деления на m фактически не само число, а его запись в соответствующей системе счисления. Поэтому признак равноостаточности при делении на данное фиксированное число m будет, вообще говоря, зависеть от основания системы счисления. Вместе с тем буквальная формулировка признака равноостаточности при делении на данное m в t-ичной системе счисления вполне может подходить для признака равноостаточности при делении на другое m' в системе счисления с другим основанием t'. Соответствующие примеры будут получаться из содержания теорем 19, 20 и 21.

Во избежание возможных недоразумений условимся в дальнейшем как делитель m, так и основание системы счисления t записывать («называть») в десятичной системе счисления. Так, говоря о признаке равноостаточности при делении на 12 в семеричной системе счисления, мы будем под 12 понимать именно число $3 \cdot 4$, а не число $3 \cdot 3$ (как это было бы, если бы число 12 рассматривалось как запись в семеричной системе счисления).

В качестве первого примера найдем признак равноостаточности при делении на 5 в десятичной системе счисления.

Пусть A — натуральное число. Представим A в виде $10a + b$ (b — последняя цифра числа A) и положим

$$f_1(A) = \begin{cases} b, & \text{если } A \geqq 10, \\ b - 5, & \text{если } 5 \leqq A < 10, \\ \text{не определено}, & \text{если } A < 5. \end{cases}$$

Читатель сам может проверить, что так определенная функция удовлетворяет условиям а)—г) п. 10.

Таким образом, для нахождения остатка от деления некоторого числа на 5 достаточно взять последнюю цифру этого числа. Если эта цифра меньше пяти, то она и будет искомым остатком; в противном случае от нее следует отнять 5. Заметим, что применение этого признака равноостаточности к любому числу приводит к построению последовательности типа (3.4), состоящей не более чем из трех членов.

Разумеется, целью всех проведенных рассуждений является не обнаружение известного всем «признака делимости» на 5, а получение его тем именно единообразным приемом, который был описан в п. 10.

Задача 31. Указать и проанализировать аналогичные признаки равноостаточности при делении на 2, 4, 8, 10, 16, 20 и 25 в десятичной системе счисления.

Задача 32. Указать и проанализировать аналогичные признаки равноостаточности при делении:

а) на 9 и 27 в троичной системе счисления;

б) на 8, 9, 16, 18, 24, 36, 48 и 72 в двенадцатеричной системе счисления.

Задача 33. Представим натуральное число A в виде

$$10^k a + b \quad (0 \leqq b < 10^k)$$

и положим

$$f(A) = \begin{cases} b, & \text{если } A \geqq 10^k, \\ \text{остатку от деления } A \text{ на } m, & \text{если } m \leqq A < 10^k, \\ \text{не определено}, & \text{если } A < m. \end{cases}$$

Для каких чисел m такой алгорифм при некотором k является признаком равноостаточности?

Теорема 21. *Представим произвольное натуральное число A в виде $at^k + b$, где $0 \leqq b < t^k$, и положим*

$$f(A) = \begin{cases} b, & \textit{если } A \geqq t^k, \\ b - m, & \textit{если } m \leqq A < t^k, \\ \textit{не определено}, & \textit{если } A < m. \end{cases}$$

Чтобы для данной функции f алгорифм построения последовательности (3.4) *по правилу* (3.5) *был признаком равноостаточности при делении на m, необходимо и достаточно, чтобы было $t^k \vdots m$.*

13. В качестве второго примера рассмотрим признак равноостаточности при делении на 3 в десятичной системе счисления.

Запись натурального числа A в десятичной системе счисления имеет вид

$$a_n 10^n + a_{n-1} 10^{n-1} + \ldots + a_1 \cdot 10 + a_0,$$

где

$$0 \leqq a_i < 10 \quad \text{для} \quad i = 0,\ 1,\ \ldots,\ n.$$

Положим

$$f_2(A) = \begin{cases} a_0 + a_1 + \ldots + a_{n-1} + a_n, & \text{если } A \geqq 10, \\ \text{остатку от деления } A \text{ на 3}, & \text{если } 3 \leqq A < 10, \\ \text{не определено}, & \text{если } A < 3. \end{cases}$$

Задача 34. Проверить, что функция $f_2(x)$ удовлетворяет условиям а)—г) и определяет тем самым некоторый признак равноостаточности при делении на 3.

Задача 35. Применить построенный признак равноостаточности при делении на 3:

а) к числам 858 773 и 789 988;

б) к числу, десятичная запись которого состоит из 4444 четверок.

Задача 36. Указать и проанализировать аналогичные признаки равноостаточности при делении на 7, 9, 11, 13 и 37 в десятичной системе счисления.

Задача 37. Указать и проанализировать признаки равноостаточности при делении:

а) на 2, 4 и 8 в троичной системе счисления;

б) на 2, 4 и 8 в семеричной системе счисления.

Теорема 22. *Представим произвольное натуральное число A в виде*

$$a_n t^{kn} + a_{n-1} t^{k(n-1)} + \ldots + a_1 t^k + a_0,$$

где

$$0 \leqq a_i < t^k \quad \textit{при} \quad i = 0,\ 1,\ \ldots,\ n,$$

и положим

$$f(A) = \begin{cases} a_0 + a_1 + \ldots + a_{n-1} + a_n, & \textit{если} \quad A \geqq t^k, \\ A - m, & \textit{если} \quad m \leqq A < t^k, \\ \textit{не определено}, & \textit{если} \quad A < m. \end{cases}$$

Тогда, для того чтобы порождаемый функцией f алгорифм построения последовательности (3.4) *по правилу* (3.5) *был признаком равноостаточности при делении на m, необходимо и достаточно, чтобы было* $(t^k - 1) \vdots m$.

Задача 38. Указать подпадающие под эту теорему признаки равноостаточности для чисел, записанных в шестеричной, семеричной, девятеричной и тринадцатеричной системах счисления.

Теорема 23. *Пусть A — натуральное число, представленное в виде*

$$a_n t^{kn} + a_{n-1} t^{k(n-1)} + \ldots + a_1 t^k + a_0,$$

где

$$0 \leqq a_i < t^k \quad \textit{при} \quad i = 0,\ 1,\ \ldots,\ n.$$

Положим

$$f(A) = \begin{cases} a_0 - a_1 + a_2 - \ldots \pm a_n, & \textit{если } A \geqq t^k, \\ \textit{остатку от деления } A \textit{ на } m, & \textit{если } m \leqq A < t^k, \\ \textit{не определено}, & \textit{если } A < m. \end{cases}$$

Тогда, для того чтобы порождаемый функцией f алгорифм построения последовательности (3.4) *по правилу* (3.5) *был признаком равноостаточности при делении на m, необходимо и достаточно, чтобы было* $(t^k + 1) \vdots m$.

Задача 39. Указать подпадающие под эту теорему признаки равноостаточности для чисел, записанных в троичной, пятеричной, восьмеричной и десятичной системах счисления.

14. Во многих задачах несущественна не только величина неполного частного от деления одного числа на другое, но также и величина остатка от деления, а интересно только, обращается этот остаток в нуль или нет, т. е. делится или нет первое число на второе. После сказанного в п. 1 ясно, как подходить к задачам такого рода.

Назовем числа a и b *равноделимыми* при делении на m, если либо и a, и b делятся на m, либо на m ни a, ни b не делятся.

Задача 40. Каково бы ни было m, любые равноостаточные при делении на m числа являются равноделимыми на m. Показать на примере, что обратное неверно.

Задача 41. Для каких m из равноделимости двух чисел при делении на m следует их равноостаточность при этом делении?

Задача 42. Доказать, что отношение равноделимости при делении на данное число m является эквивалентным отношением и разбивает множество целых чисел на два класса.

Задача 43. Будет ли справедлива для равноделимых чисел теорема 20? Ее следствие?

15. Пусть нужно выяснить делимость на m числа A. Будем строить последовательность убывающих натуральных чисел

$$A = A_0,\ A_1,\ A_2,\ \ldots, \tag{3.6}$$

равноделимых с A при делении на m с остатком. Способ построения последовательности (3.6) выберем такой, чтобы за всяким членом этой последовательности, бóльшим или равным m по абсолютной величине, следовал еще хотя бы один член. Если при этом последний член (3.6) будет равен нулю, то A делится на m, а если не равен нулю, то не делится.

Всякий способ построения последовательности (3.6) назовем *признаком делимости* на m.

Задача 44. Доказать, что всякий признак равноостаточности при делении на m является признаком делимости на m.

Очевидно, признаки делимости должны быть алгорифмичными, т. е. удовлетворять таким же условиям определенности, массовости и результативности, что и признаки равноостаточности.

Нетрудно проверить (это предоставляется читателю), что при помощи всякой функции $f(x)$, удовлетворяющей условиям а)—в) из п. 10 и условию

г*) если $f(x)$ имеет смысл, то числа x и $f(x)$ равноделимы на m,

можно построить признак делимости на m точно таким же образом, как строился признак равноостаточности при делении на m по всякой функции, удовлетворяющей условиям а)—г).

Найдем несколько признаков делимости.

Согласно теореме 16 достаточно уметь определять делимость чисел на числа вида p^α (т. е. на степени простых чисел).

16. Признак делимости на 7 в десятичной системе счисления. Пусть A — натуральное число. Представим A в виде $10a + b$, где $0 \leqq b < 10$, как это уже делалось раньше. Положим

$$f_3(A) = \begin{cases} |a - 2b|, & \text{если } A \geqq 19, \\ \text{остатку от деления } A \text{ на } 7, & \text{если } 7 \leqq A < 19, \\ \text{не определено,} & \text{если } A < 7. \end{cases}$$

Задача 45. Проверить выполнение для функции $f_3(A)$ условий а)—в) и г*).

Функция $f_3(A)$ дает нам известный признак делимости на 7: число $10a + b$ $(0 \leqq b < 10)$ делится на 7 тогда и только тогда, когда на 7 делится число $a - 2b$; полученное число снова проверяется этим же способом на делимость на 7 и т. д.

Задача 46. Доказать, что полученный признак делимости на 7 не является признаком равноостаточности при делении на 7 с остатком.

17. Признак делимости на 13. Представим натуральное число A в виде $10a + b$ и положим

$$f_4(A) = \begin{cases} a + 4b, & \text{если } A \geqq 40, \\ \text{остатку от деления } A \text{ на } 13, & \text{если } 13 \leqq A < 40, \\ \text{не определено}, & \text{если } A < 13. \end{cases}$$

Задача 47. Проверить выполнение условий а)—в) и г*) для функции $f_4(x)$ и сформулировать полученный признак делимости на 13.

Задача 48. К каким последствиям приведет замена в определении функции f_4 числа 40 на меньшее?

Задача 49. По аналогии с построенными признаками делимости на 7 и 13 построить аналогичные признаки делимости на 17, 19, 23, 29 и 31.

Задача 50. Построить два признака делимости на 49.

18. Признаки делимости того же типа имеются и для чисел, записанных в других, недесятичных системах счисления.

Признак делимости на 11 в шестеричной системе счисления. Представим натуральное число A в виде $6a + b$, где $0 \leqq b < 6$ (в соответствии со сказанным выше все рассуждения ведутся с употреблением обозначений и названий чисел в десятичной системе счисления), и положим

$$f(A) = \begin{cases} a + 2b, & \text{если } A \geqq 11, \\ 0, & \text{если } A = 11, \\ \text{не определено}, & \text{если } A < 11. \end{cases}$$

Задача 51. Проверить соблюдение условий а)—в) и г*) для функции f и сформулировать полученный признак делимости.

Задача 52. По аналогии с только что построенным признаком делимости построить признаки делимости:

а) на 5 в семеричной системе счисления;

б) на 7 в одиннадцатеричной системе счисления;

в) на 17 в двенадцатеричной системе счисления.

19. В предыдущих пунктах этого параграфа мы познакомились с большим количеством самых разнообразных признаков равноостаточности и признаков делимости. Практической целью построения всех этих признаков является получение удобно работающих алгорифмов нахождения остатков при делении на некоторые определенные числа (признаки равноостаточности) или алгорифмов, обнаруживающих, равны эти остатки нулю или нет (признаки делимости). Насколько же мы осуществили поставленную цель?

Некоторые признаки равноостаточности, такие, как при делении на 2, 3, 5, 10 в десятичной системе счисления (и вообще — на делитель степени основания системы счисления), действительно оказались весьма практичными и удобными. Применение других признаков связано с более или менее громоздкими вычислениями.

Естественно поэтому искать и применять такие признаки делимости и равноостаточности, использование которых приводит к цели по возможности более простым путем.

Одна из трудностей, с которой мы сталкиваемся при такого рода попытках, состоит в том, что мы должны уметь простоту (или, наоборот, сложность) применения того или иного признака оценивать некоторым числом. В качестве такой числовой характеристики можно, например, взять число арифметических действий над однозначными числами, которые необходимо произвести в процессе применения данного признака к тому или иному числу.

К сожалению, всякая такая характеристика объема вычислений в сильной мере зависит от индивидуальных свойств того числа, делимость которого мы хотим испытать.

Так, например, очень легко убедиться в том, что остаток от деления числа 31 025 на 8 есть 1. Для этого достаточно найти остаток от деления на 8 числа 25. Но для нахождения остатка от деления 30 525 на 8 следует разделить на 8 с остатком число 525, а это

уже требует бóльшего числа выкладок (безразлично, проводимых в уме или на бумаге).

В качестве другого примера рассмотрим признак равноостаточности при делении на 37 (см. задачу 36). Остаток от деления на 37 числа 10 014 023 находится сложением $10 + 14 + 23$ и делением полученной суммы на 37. Остаток, как легко видеть, равен 10. Однако немногие смогут в уме применить этот признак равноостаточности к числу 782 639 485.

Поэтому, говоря об удобстве использования признаков делимости и равноостаточности, нам следовало бы отвлечься от сложностей индивидуальных испытаний чисел на делимость и оценивать возможности каждого признака «в среднем». При таком подходе мы могли бы надеяться точно сформулировать меру сложности признака делимости или равноостаточности и даже найти наиболее экономный в этом смысле признак. К сожалению, мы лишены здесь возможности развивать эту исключительно трудную сторону вопроса более подробно.

Но это еще не все. Имеется и другая трудность в оценке качества признаков делимости и равноостаточности. Она заключается в том, что такая оценка может производиться с различных точек зрения: кроме упомянутого числа арифметических операций над однозначными числами мы можем считать простым тот из признаков, применение которого (к каждому числу или «в среднем») требует меньшего числа шагов, т. е. более короткой последовательности (3.4) (или соответственно последовательности (3.6)); можно, наконец, за простоту признака принимать так или иначе понимаемую простоту (например, запоминаемость) функции f из (3.5). В результате мы оказываемся в условиях «многокритериальной оценки», с которой мы по другому поводу уже встречались в п. 9 § 1.

§ 4. ОБЩИЕ ПРИЗНАКИ РАВНООСТАТОЧНОСТИ И ДЕЛИМОСТИ

1. Все построенные выше признаки равноостаточности, а также признаки делимости выглядят несколько искусственно, и на первый взгляд может показаться, что эти признаки или, во всяком случае, некоторые из них были найдены случайно или же в результате проб и испытаний. На самом деле это не так. Оказывается, существуют способы построения признаков равноостаточности и делимости на любое наперед заданное число. Они называются *общими признаками равноостаточности* или соответственно *общими признаками делимости.*

Общие признаки равноостаточности являются способами получения конкретных признаков равноостаточности. Поэтому конкретные признаки равноостаточности можно считать теми результатами, к которым приводят общие признаки. С этой точки зрения общие признаки равноостаточности относятся к конкретным совершенно так же, как конкретный признак равноостаточности относится к результату своего применения к некоторому числу, т. е. к остатку от деления данного числа a на данное число m.

Общие признаки равноостаточности и делимости напоминают алгорифмы, и притом алгорифмы довольно своеобразные: их итогами, результатами должны быть снова алгорифмы, именно: конкретные признаки равноостаточности или делимости.

Однако, для того чтобы говорить об общих признаках равноостаточности и делимости как об алгорифмах, мы должны убедиться в том, что они обладают нужными условиями определенности, массовости и результативности.

Говоря подробнее, указывая общий признак делимости (равно как и общий признак равноостаточности), мы должны проверить выполнение следующих условий. Во-первых, по всякому числу m он должен действительно давать признак делимости (равноостаточности) на это число. Он должен, так сказать, «перерабатывать» каждое натуральное число m в соответствующий признак. Именно в этом и состоит его результативность. Во-вторых, общий признак должен быть определенным, т. е., примененный к заданному числу m, он должен приводить вполне определенным способом к вполне определенному конкретному признаку делимости (равноостаточности) на это число. Наконец, в-третьих, признак должен быть массовым, т. е. действительно общим, и давать признаки делимости или равноостаточности на любое наперед заданное натуральное число.

В этом смысле описанный в п. 6 § 3 способ задания признака равноостаточности, а также описанный в п. 9 § 3 способ нахождения признаков делимости не являются общими признаками. Действительно, указание функций, обладающих нужными свойствами, является процессом, не удовлетворяющим пока ни одному из требований определенности, массовости и результативности.

В самом деле, эти способы не дают нам никакой гарантии в том, что нужная функция будет найдена; значит, они лишены результативности. Далее, если требуемая функция и существует, к ней можно прийти разными путями, не говоря уже о том, что таких функций может оказаться несколько. Значит, эти способы лишены определенности. Наконец, ему не хватает и массовости, так как, быть может, требуемых функций для тех или иных конкретных значений m нам найти не удастся. Сам способ нам, во всяком случае, ничего об этом не говорит. Таким образом, для того чтобы описанный процесс стал алгорифмом, он должен быть еще дополнен точными указаниями, гарантирующими построение вполне определенной функции f_m для каждого конкретного числа m.

Эта задача «алгорифмизации» построения признаков равноостаточности и признаков делимости может быть решена, и даже без особого труда, а общие признаки делимости известны уже давно.

Один такой общий признак равноостаточности фактически уже был нами построен в п. 11 § 1 при выяснении вопроса о делении с остатком. Мы его можем сформулировать так: каждому целому положительному числу m ставится в соответствие процесс последовательного вычитания этого числа m до получения числа, меньшего чем m (см. последнюю фразу п. 1 § 3). Ясно, что такое соответствие обладает необходимыми свойствами определенности (мы точно знаем, что́ ставится в соответствие числу m: процесс последовательного вычитания этого числа m), массовости (процесс последовательного вычитания можно пытаться применить к любому m) и результативности (такая попытка обязательно приведет к успеху). Однако практическая ценность описанного общего признака равноостаточности весьма невелика.

Некоторое усовершенствование общего признака равноостаточности, основанного на последовательном вычитании, приводит к известному процессу деления целых чисел «углом». Этот процесс деления тоже может рассматриваться как общий признак равноостаточности. Нелишним будет напомнить, что подавляющее большинство людей пользуется при нахождении остатков от деления именно этим признаком. При этом рассуждение ведется по следующей схеме, которую мы воспроизведем в двух вариантах: на обычном житейском языке и на языке алгорифмов.

На житейском языке	На языке алгорифмов
1) Я должен найти остаток от деления данного a на данное m;	Общий признак равноостаточности начинает переработку числа m;
2) для этого я буду делить на m;	общий признак «выдает» результат переработки числа m: конкретный признак равноостаточности при делении на m, заключающийся в непосредственном делении на m с остатком;
3) вот я начинаю делить a на m...	полученный конкретный признак начинает переработку числа a: деление на m с остатком;
4) ...делю и получаю остаток.	конкретный признак приводит к цели: к остатку от деления a на m.

В этом рассуждении первые три шага уже очень просты, и поэтому не приходится удивляться, что четвертый шаг, состоящий в фактическом выполнении деления, оказывается таким громоздким. Цель создания общих признаков равноостаточности и делимости и состоит в разгрузке четвертого шага путем усовершенствования второго. Именно это и имеют обычно в виду, когда говорят об общих признаках делимости и равноостаточности.

2. Исторически первым общим признаком делимости (точнее, даже признаком равноостаточности) является следующий, предложенный знаменитым французским математиком Паскалем еще в середине XVII столетия. Сущность этого признака такова.

Пусть m — натуральное число. Составим последовательность чисел

$$r_1,\ r_2,\ r_3,\ \ldots, \tag{4.1}$$

полагая

r_1 равным остатку от деления 10 на m,

r_2 равным остатку от деления $10r_1$ на m,

r_3 равным остатку от деления $10r_2$ на m

и т. д.

Представим теперь произвольное натуральное число A в виде

$$10^n a_n + 10^{n-1}a_{n-1} + \ldots + 10a_1 + a_0$$

и определим функцию

$$F_m(A) = \begin{cases} a_0 + r_1a_1 + r_2a_2 + \ldots + r_na_n, & \text{если } 10^n \geqq m, \\ \text{остатку от деления } A \text{ на } m, & \text{если } 10^n < m \leqq A, \\ \text{не определено,} & \text{если } A < m. \end{cases}$$

Задача 53. Проверить, что функция F_m при любом m удовлетворяет условиям а) — г) из п. 10 § 3.

Итак, нами построен признак равноостаточности при делении на произвольное m, т. е. некоторый общий признак равноостаточности.

Задача 54. Сформулировать получаемые из общего признака равноостаточности Паскаля признаки равноостаточности при делении:

а) на 2, 5 и 10;

б) на 4, 20 и 25;

в) на 3 и 9;
г) на 11;
д) на 7.

Задача 55. Пусть в последовательности (12)

r_1 есть остаток от деления 100 на m,

r_2 есть остаток от деления $100r_1$ на m,

r_3 есть остаток от деления $100r_2$ на m

и т. д.

Вывести отсюда общий признак равноостаточности, аналогичный общему признаку равноостаточности Паскаля.

Задача 56. Вывести общий признак равноостаточности в t-ичной системе счисления, аналогичный признаку Паскаля.

3. В п. 19 § 3 мы говорили о сравнительных качествах признаков делимости (или равноостаточности) на данное число. Так как общий признак делимости должен давать нам признаки делимости на любое натуральное число, то неудивительно, что он может для различных чисел приводить к признакам делимости весьма различного качества.

Так, например, общий признак Паскаля наряду с вполне приемлемыми признаками равноостаточности при делении на 3 и 11 дает весьма громоздкий и неудобный к применению признак равноостаточности при делении на 7 (см. задачу 54, д)).

В связи с этим по поводу общих признаков делимости и равноостаточности можно высказать соображения, подобные тем, которые производились в п. 19 § 3 при обсуждении качества конкретных признаков делимости и равноостаточности. В этом смысле наилучшим общим признаком делимости (равноостаточности) должен считаться тот, который в применении к любому наперед заданному целому положительному m дает наилучший признак делимости (равноостаточности) на это m. Читатель (особенно в свете сказанного в п. 19 § 3) должен отдавать себе отчет в том, что задачи нахождения наилучшего общего признака делимости или равноостаточности далеки не только от своего решения, но даже от строгой постановки.

§ 5. ДЕЛИМОСТЬ СТЕПЕНЕЙ

1. Начнем с описания процесса, который можно было бы назвать «очень общим признаком равноостаточности».

Пусть k — некоторое натуральное число, а r есть остаток от деления t^k на m:

$$t^k = mq + r \quad (0 \leqq r < m).$$

По следствию теоремы 20 (см. п. 3 § 2) при любом n числа r^n и t^{kn} при делении на m также должны быть равноостаточными.

Составим теперь для произвольного числа A его разбиение на k-значные «грани» справа налево, т. е. представим его в виде

$$A = a_n t^{kn} + a_{n-1} t^{k(n-1)} + \ldots + a_1 t^k + a_0,$$

где

$$0 \leqq a_i < t^k \quad \text{при} \quad i = 0, 1, \ldots, n.$$

Положим теперь

$$f(A) =$$

$$= \begin{cases} a_n r^n + a_{n-1} r^{n-1} + \ldots + a_1 r + a_0, & \text{если } A \geqq t^k, \\ \text{остатку от деления } A \text{ на } m, & \text{если } m \leqq A < t^k, \\ \text{не определено,} & \text{если } A < m. \end{cases}$$

Ясно, что, как и ранее в аналогичных случаях, процесс построения чисел

$$A_0 = A, \quad A_1 = f(A_0), \quad A_2 = f(A_1), \ldots$$

является признаком равноостаточности.

Задача 57. Убедиться все-таки в том, что это действительно так.

Задача 58. Полагая $t = 10$ и $k = 2$, найти остаток от деления числа 1 048 576 на 7.

Задача 59. Убедиться в том, что только что описанный признак равноостаточности является лишь более явной формой того обобщения признака Паскаля, которое было упомянуто в задаче 56.

2. Говоря формально, при составлении в п. 1 общего признака равноостаточности мы пользовались свойствами степеней, относящимися к их делимости. Однако вопрос о делимости степеней по существу является вопросом о делимости некоторых произведений. Поэтому и решить этот вопрос в принципе удалось на основе результатов § 2. Вместе с тем практическая реализация полученного признака равноостаточности для тех или иных комбинаций значений чисел t и m может приводить к крупным значениям k и r, так что вычисление значений функции f может потребовать выполнения значительных вычислений, возможно даже превосходящих по объему выкладки по непосредственному делению на m.

Ясно, что вычисление значений функции f оказывается тем проще, чем меньшими будут значения чисел k и r. Разумеется, наиболее удобным оказывается в этом отношении тот случай, когда $r = 1$. Тогда значение f получается в результате выполнения наименее трудоемкого действия: сложения.

Согласно теореме 22 этот случай ($r = 1$) имеет место тогда и только тогда, когда $(t^k - 1) \vdots m$ или, иными словами, когда t^k при делении на m дает в остатке 1. Встает вопрос: найдется ли при данных t и m такое k, что $(t^k - 1) \vdots m$?

Все сказанное приводит к необходимости заняться изучением делимости степеней несколько более подробно.

3. Расширим несколько наши познания в области теории чисел.

Теорема 24 (теорема Ферма). *Если число p простое, то разность $a^p - a$ делится на p.*

Не следует путать эту так называемую «малую теорему Ферма» с «великой теоремой Ферма». Последняя утверждает, что при целом $n > 2$ не существует таких целых a, b и c, что $a^n + b^n = c^n$. Несмотря на многочисленные попытки, великая теорема Ферма до сих пор не доказана и не опровергнута.

Следствие. Если p простое и a не делится на p, то $a^{p-1} - 1$ делится на p.

Задача 60. Привести пример, показывающий, что как теорема 24, так и ее следствие для составного p, вообще говоря, неверны.

Задача 61. Доказать теорему Ферма, опираясь на результат задачи 26.

Пусть натуральное число m имеет каноническое разложение:

$$m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}; \tag{5.1}$$

положим

$$\varphi(m) = p_1^{\alpha_1 - 1}(p_1 - 1)\, p_2^{\alpha_2 - 1}(p_2 - 1) \dots p_k^{\alpha_k - 1}(p_k - 1). \tag{5.2}$$

Формулы (5.1) и (5.2) ставят в соответствие каждому натуральному числу m некоторое вполне определенное число $\varphi(m)$. Это значит, что мы можем говорить о функции φ натурального аргумента.

Определение. Определенная выше функция φ называется *функцией Эйлера.*

Функция Эйлера играет исключительно важную роль во многих вопросах теории чисел. Даже в этой книжке будет указано несколько применений этой функции.

Теорема 25. *При взаимно простых m_1 и m_2 имеет место равенство*

$$\varphi(m_1 m_2) = \varphi(m_1)\,\varphi(m_2).$$

Задача 62. Вычислить $\varphi(12)$, $\varphi(120)$, $\varphi(1000)$.

Задача 63. Определить все числа m, для которых:

а) $\varphi(m) = 10$;

б) $\varphi(m) = 8$.

Задача 64. Доказать, что не существует такого m, для которого $\varphi(m) = 14$.

Задача 65. Показать, что $\varphi(m)$ равно числу натуральных чисел, взаимно простых с m и меньших m.

Это свойство функции Эйлера является чрезвычайно важным. Его часто принимают за определение этой функции.

Теорема 26 (теорема Эйлера). *Если числа a и m взаимно просты, то $a^{\varphi(m)} - 1$ делится на m.*

Остатки при делении одного и того же делимого на различные делители связаны между собой достаточно сложным образом. Из теоремы Эйлера можно получить принципиально важную для нас зависи-

мость между остатками от деления на взаимно простые множители и остатками от деления на их произведение.

Задача 66. Пусть $(m_1, m_2) = 1$, а a_1 и a_2 — числа, равноостаточные с A при делении соответственно на m_1 и m_2. Тогда равноостаточным с A при делении на $m_1 m_2$ будет число

$$(a_1 m_2 + a_2 m_1)(m_1 + m_2)^{\varphi(m_1 m_2)-1}.$$

4. На основании установленных фактов мы можем сформулировать общий признак равноостаточности для произвольного делителя m в произвольной системе счисления t в той явной и достаточно удобной форме, о которой говорилось в п. 1.

Напомним снова, что всякий признак равноостаточности есть алгорифм, т. е. некоторый процесс, и потому всякое его описание должно носить характер развивающегося повествования.

Итак, пусть нам даны числа m и t. Представим m в виде такого произведения $m = m_1 m_2$, что $(m_1, t) = 1$ и для некоторого показателя k имеет место делимость $t^k \vdots m_2$. Согласно теореме 18 такое представление возможно. В силу задачи 66 вопрос о равноостаточности при делении на $m_1 m_2$ может быть сведен к аналогичным вопросам для деления на m_1 и m_2. Но признак равноостаточности для деления на m_2 содержится в теореме 21, а признак равноостаточности для деления на m_1 — в теореме 22. После применения этих признаков равноостаточности следует воспользоваться результатом задачи 66.

Например, в случае нахождения признака равноостаточности при делении на 12 в десятичной системе счисления, очевидно, $m_1 = 3$, $m_2 = 4$ и $k = 2$.

Описанный процесс является общим признаком равноостаточности в том смысле, что по любому m он выдает некоторый конкретный признак равноостаточности. Это вытекает из алгорифмичности представления числа m в форме, указываемой в теореме 18, а сама эта алгорифмичность следует из алгорифмичности построения канонического разложения чисел (см п. 9 § 3).

Нам остается сформулировать в явном виде указанный признак равноостаточности при делении на m_1, пользуясь возможностью определить показатель k на основании теоремы Эйлера.

5. Применяя доказанные теоремы, построим несколько общих признаков делимости и равноостаточности.

Фиксируем натуральное m и представим число A в виде

$$A = a_0 + a_1 10^{\varphi(m)} + a_2 10^{2\varphi(m)} + \ldots + a_k 10^{k\varphi(m)},$$

где

$$0 \leqq a_0,\ a_1,\ a_2,\ \ldots,\ a_k \leqq 10^{\varphi(m)},$$

т. е. все a_i $(i = 0, 1, \ldots, k)$ являются $\varphi(m)$-значными числами.

Функция

$$F(A) =$$

$$= \begin{cases} a_0 + a_1 + \ldots + a_k, & \text{если } A \geqq 10^{\varphi(m)}, \\ \text{остатку от деления } A \text{ на } m, & \text{если } m \leqq A < 10^{\varphi(m)}, \\ \text{не определено}, & \text{если } A < m, \end{cases}$$

определяет, как нетрудно проверить, некоторый общий признак равноостаточности.

Задача 67. Проверить это обстоятельство.

Теорема 27. *Если числа a и m взаимно просты, а числа k_1 и k_2 равноостаточны при делении на $\varphi(m)$, то числа a^{k_1} и a^{k_2} равноостаточны при делении на m.*

Задача 68. Сформулировать получаемые на основе этого общего признака равноостаточности конкретные признаки равноостаточности при делении на 7, 11 и 13.

Задача 69. Сформулировать аналогичный общий признак равноостаточности для произвольной t-ичной системы счисления. Убедиться в том, что получаемый так общий признак равноостаточности по своей формулировке не зависит от основания системы счисления t.

Задача 70. Доказать, что $(n^{13} - n) \vdots 2730$.

6. Построенный общий признак равноостаточности не является во многих случаях, так сказать, «достаточно экономным», так как число $\varphi(m)$ может, вообще говоря, оказаться довольно большим. Поэтому, с одной стороны, при пользовании этим признаком приходится складывать большие числа, а с другой стороны, $\varphi(m)$-значные числа при этом приходится делить на m непосредственно (или же пользоваться каким-нибудь другим признаком делимости

и равноостаточности). Желательно поэтому попытаться взять вместо $\varphi(m)$ другой, меньший показатель. В ряде случаев это удается сделать. Например, при $m = 37$ вместо $\varphi(m) = 36$ можно взять показатель 3, ибо 1000 при делении на 37 дает в остатке единицу; при $m = 11$ вместо $\varphi(m) = 10$ можно взять показатель 2 и т. д.

Определение. Наименьшее число δ, для которого a^δ при делении на m с остатком дает в остатке 1, называется *показателем, которому принадлежит число a* при делении на m с остатком.

Его часто называют также *показателем, которому принадлежит число a по модулю m.*

Очевидно, каковы бы ни были взаимно простые числа a и m, показатель δ, которому принадлежит a при делении на m, не превосходит $\varphi(m)$. Этот показатель и можно взять вместо $\varphi(m)$ в формулировке общего признака равноостаточности из п. 5.

Задача 71. Модифицировать построенный общий признак равноостаточности, используя вместо $\varphi(m)$ показатель, которому принадлежит 10 при делении на m с остатком.

Задача 72. То же для t-ичной системы счисления.

7. Показатель, которому принадлежит число a при делении на m, может, вообще говоря, быть и равным $\varphi(m)$. Например, последовательностью остатков от деления степеней числа 2 на 11 будет

$$2,\ 4,\ 8,\ 5,\ 10,\ 9,\ 7,\ 3,\ 6,\ 1,$$

так что при делении на 11 число 2 принадлежит показателю 10. Значит, для применения признака равноостаточности из п. 5 в этом случае приходится брать $k = 10 = \varphi(11)$.

Однако во многих случаях удается обходиться показателем $\frac{1}{2}\varphi(m)$. Пусть, например, m есть степень простого числа: $m = p^\alpha$ и $p \neq 2$. Тогда $\varphi(m) = p^{\alpha-1}(p-1)$, и теорема Эйлера приобретает вид: для $(a, p)=1$ должно быть $\left(a^{p^{\alpha-1}(p-1)} - 1\right) \vdots\ p^\alpha$. Так как число $p^{\alpha-1}(p-1)$ четное, последнее делимое есть разность квадратов, и мы имеем

$$\left(a^{\frac{1}{2}p^{\alpha-1}(p-1)} + 1\right)\left(a^{\frac{1}{2}p^{\alpha-1}(p-1)} - 1\right) \vdots\ p^\alpha.$$

Так как $p \neq 2$, оба сомножителя одновременно на p делиться не могут. Значит, на p^α делится либо $a^{\frac{1}{2}\varphi(m)} + 1$, либо $a^{\frac{1}{2}\varphi(m)} - 1$. В первом случае мы оказываемся в условиях

теоремы 23 с $k = \frac{1}{2}\varphi(m)$, а во втором — в условиях теоремы 22 с тем же $k = \frac{1}{2}\varphi(m)$.

8. Применения функции Эйлера и теоремы Эйлера не ограничиваются признаками делимости и равноостаточности. Например, при их помощи можно решать уравнения в целых числах.

Теорема 28. *Если числа a и b взаимно просты, то уравнение*

$$ax + by = c \qquad (5.3)$$

всегда разрешимо в целых числах, и целыми его решениями будут все пары чисел (x_t, y_t), где

$$x_t = ca^{\varphi(b)-1} + bt,$$

$$y_t = c\frac{1 - a^{\varphi(b)}}{b} - at$$

(t — любое целое число).

Задача 73. Доказать теорему, аналогичную теореме 28, не предполагая взаимной простоты чисел a и b.

Задача 74. Найти способ решения уравнений вида (5.3) в целых числах на основе результата задачи 29, б).

Задача 75. Решить в целых числах уравнения:

а) $5x + 7y = 9$;

б) $25x + 13y = 8$.

9. Теорема 29. *Пусть m взаимно просто с 10 и k равноостаточно с $10^{\varphi(m)-1}$ при делении на m. Тогда числа*

$$10a + b \quad \text{и} \quad a + kb$$

равноделимы на m.

Опираясь на эту теорему, можно построить следующий общий признак делимости. Обозначим через k остаток от деления $10^{\varphi(m)-1}$ на m с остатком, представим произвольное число A в виде

$$10a + b \qquad (0 \leqq b < 10)$$

и положим

$$F(A) = \begin{cases} a + kb, & \text{если } A > a + kb, \\ \text{остатку от деления } A \text{ на } m, & \text{если } m \leqq A < a + kb, \\ \text{не определено}, & \text{если } A < m. \end{cases}$$

Если k велико (близко к m), то вместо него в формулировке соответствующего признака целесообразно брать $k - m$.

Задача 76. Проверить для функции F выполнение условий а) — в) из п. 10 § 3 и г *) из п. 15 § 3.

Задача 77. На основании только что построенного общего признака делимости вывести конкретные признаки делимости на числа 17, 19, 27, 29, 31 и 49.

Задача 78. Построить аналогичный общий признак делимости, представляя произвольное натуральное число в виде

$$100a + b \quad (0 \leqq b < 100),$$

и вывести из него конкретные признаки делимости на 17, 43, 49, 67, 101, 199.

Задача 79. Построить аналогичный общий признак делимости в t-ичной системе счисления.

Задача 80. На основании построенного общего признака делимости вывести конкретные признаки делимости:

а) на число 21 в восьмеричной системе счисления;

б) на число 31 в двенадцатеричной системе счисления.

ДОКАЗАТЕЛЬСТВА ТЕОРЕМ

1. Достаточно заметить, что $a = a \cdot 1$.

2. По условию, найдутся такие d_1 и d_2, что $a = bd_1$ и $b = cd_2$. Но тогда $a = cd_1d_2$, т. е. $a \vdots c$.

3. Мы имеем $a = bc_1$ и $b = ac_2$, откуда следует, что $a = ac_1c_2$, т. е. $c_1c_2 = 1$. Так как числа c_1 и c_2 по условию целые, должно быть либо $c_1 = c_2 = 1$, либо $c_1 = c_2 = -1$. В первом из этих случаев $a = b$, а во втором $a = -b$.

4. Пусть $a = bc$. Если $|c| \geqq 1$, то, поскольку $|b| > |a|$, должно быть и $|bc| > |a|$, что, однако, противоречит предположенному. Значит, $|c| < 1$, а так как по условию число c целое, должно быть $c = 0$, а потому и $a = 0$.

5. Очевидно, из $a = bc$ следует $|a| = |b||c|$, а из $|a| = |b||c|$ следует $a = bc$ или $a = b(-c)$, причем числа c, $-c$ и $|c|$ целые или нет одновременно.

6. В самом деле, пусть

$$a_1 = bc_1,$$
$$a_2 = bc_2,$$
$$\cdots$$
$$a_n = bc_n,$$

где все числа $c_1, c_2, \ldots, c_n$ целые. Сложив все эти равенства почленно, получим

$$a_1 + a_2 + \ldots + a_n = b(c_1 + c_2 + \ldots + c_n).$$

В скобках стоит целое число, что и доказывает требуемое.

8. Доказательство ведется от противного. Предположим, что простых чисел конечное число, так что все они могут быть выписаны:

$$p_1, p_2, \ldots, p_n. \qquad (Д.1)$$

Произведение всех этих чисел обозначим через P и рассмотрим разность $P-1$. Эта разность больше каждого из простых чисел, перечисленных в списке (Д. 1), и потому не может быть простым числом. Следовательно, она делится хотя бы на одно простое число p_k. Но P также делится на p_k. Поэтому на основании следствия теоремы 6 должно быть и $1 \vdots p_k$, откуда следует, что $p_k = 1$, а это противоречит простоте числа p_k (см. с. 20).

Приведенное доказательство бесконечности множества простых чисел было найдено Евклидом (IV век до н. э.).

9. Если числа a и p взаимно просты, то теорема доказана. Если же эти числа не взаимно просты, то оба они делятся на одно и то же число, отличное от единицы. Ввиду простоты p таким числом может быть только само p. Значит, в этом случае $a \vdots p$, а это и требовалось.

10. Разделив M на m с остатком, получим

$$M = mq + r,$$

где $0 \leqq r < m$. Так как M и m делятся на a и b, по следствию теоремы 6 число r также должно делиться и на a, и на b и тем самым быть общим кратным этих чисел. Но $r < m$, а m есть наименьшее положительное общее кратное a и b. Значит, r не может являться положительным числом, так что $r = 0$. Поэтому $M \vdots m$.

11. Пусть числа a и b взаимно просты и m — их наименьшее общее кратное. Так как $ab \vdots a$ и $ab \vdots b$, по предыдущей теореме $ab \vdots m$. Пусть $ab = mk$. Положим $m = ac$. Тогда $ab = ack$, т. е. $b = ck$, так что $b \vdots k$. Точно так же убеждаемся в том, что и $a \vdots k$. Так как числа a и b по условию взаимно простые, должно быть $k = 1$, а это и означает, что $m = ab$.

12. Обозначим через m наименьшее общее кратное чисел b и c. По предыдущей теореме $m = bc$. Далее, по условию $ab \vdots c$; кроме того, очевидно, $ab \vdots b$. Значит, по теореме 10 $ab \vdots bc$, т. е. $ab = bck$ или, после сокращения на b, $a = ck$, а это и требовалось.

13. Доказательство ведется индукцией по числу сомножителей. Если сомножитель один, то теорема тривиальна. Предположим, что теорема доказана для любого произведения n сомножителей. Пусть $a_1a_2 \ldots a_na_{n+1} \vdots p$. Обозначим $a_1a_2 \ldots a_n$ через A.

Тогда $Aa_{n+1} \vdots p$. Если $a_{n+1} \vdots p$, то теорема доказана, а если нет, то по теореме 9 числа a_{n+1} и p взаимно просты. Но тогда по предыдущему $A \vdots p$. Так как A есть произведение n сомножителей, по индуктивному предположению один из них должен делиться на p. Теорема доказана.

Следствие. *Вся дробь представляет собой целое число, т. е. ее числитель делится на знаменатель.*

Будем считать, что числитель является произведением двух сомножителей: p и $1 \cdot 2 \cdot \ldots \cdot (p-1) = (p-1)!$ Ни один из сомножителей знаменателя дроби не делится на p. Следовательно, по предыдущей теореме, на p не делится и весь знаменатель. Но тогда на основании теоремы 9 он взаимно прост с p. Поэтому на знаменатель должен делиться второй сомножитель числителя. Обозначая частное от этого деления через q, мы имеем $C_p^k = pq$, и требуемое доказано.

14. Сначала докажем возможность разложения любого числа, отличного от единицы, на простые множители. Предположим, что все числа, меньшие N, могут быть так разложены. Если число N простое, то оно автоматически разлагается в произведение простых (именно, в произведение, состоящее только из одного сомножителя — самого числа N), и теорема доказана. Пусть теперь N составное, N_1 — некоторый делитель N, отличный как от N, так и от единицы, и N_2 — частное от деления N на N_1. Тогда $N = N_1 N_2$, причем, как легко проверить, $1 < N_2 < N$. Так как N_1 и N_2 меньше N, по предположению они разлагаются в произведения простых множителей. Пусть $N_1 = p_1 p_2 \ldots p_k$ и $N_2 = q_1 q_2 \ldots q_l$ — эти разложения. Тогда $p_1 p_2 \ldots p_k q_1 q_2 \ldots q_l$ является искомым разложением числа N. Возможность разложения, таким образом, доказана.

Переходим к доказательству единственности разложения. Пусть нам даны два разложения числа N на простые множители: $p_1 p_2 \ldots p_k$ и $q_1 q_2 \ldots q_l$. Очевидно,

$$p_1 p_2 \ldots p_k = q_1 q_2 \ldots q_l. \qquad (Д.2)$$

Так как $q_1 q_2 \ldots q_l$ делится на p_1, по предыдущей теореме хотя бы одно из чисел $q_1, q_2, \ldots, q_l$ делится на p_1. Пусть $q_1 \vdots p_1$ (то, что мы считаем именно первый сомножитель в (Д.2) справа делящимся на p_1,

никакого дополнительного предположения не означает, так как мы вправе переставлять сомножители местами и обозначить через q_1 именно тот из них, который делится на p_1). Так как число q_1 простое, это возможно лишь при $p_1 = q_1$. Сокращая равенство (Д.2) на p_1, получаем

$$p_2 p_3 \ldots p_k = q_2 q_3 \ldots q_l. \qquad (Д.3)$$

Аналогично предыдущему убеждаемся в том, что некоторое из чисел $q_2, q_3, \ldots, q_l$ (например, q_2) делится на p_2, и потому $p_2 = q_2$. Сокращая равенство (Д.3) на p_2, мы уменьшаем число сомножителей в его частях еще на единицу. Такой процесс сокращения, очевидно, можно продолжать до тех пор, пока мы не сократим одно из произведений полностью. Пусть первым сократится произведение, стоящее в (Д.2) слева. Произведение, стоящее в (Д.2) справа, тоже должно при этом сократиться нацело, так как в противном случае мы получили бы равенство вида

$$1 = q_{k+1} \ldots q_l,$$

которое невозможно, так как единица не делится ни на какое простое число. При этом мы получаем также, что

$$p_1 = q_1, \quad p_2 = q_2, \ldots, p_k = q_k.$$

Теорема полностью доказана.

15. Пусть $p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ и $q_1^{\beta_1} q_2^{\beta_2} \ldots q_t^{\beta_t}$ — соответственно канонические разложения чисел a и b, а d — некоторый общий делитель этих чисел. Если $d \neq 1$, то d делится на некоторое простое число p. Тогда по теореме 3 $a \vdots p$ и $b \vdots p$, так что p находится как среди чисел $p_1, p_2, \ldots, p_k$, так и среди чисел $q_1, q_2, \ldots, q_l$. Поэтому среди простых чисел, входящих в каноническое разложение a, существует хотя бы одно, входящее в каноническое разложение b.

Наоборот, если a и b взаимно просты и p входит в каноническое разложение a, то b не делится на p, так что p не может входить в каноническое разложение b.

16. Необходимость. Так как $a \vdots p_i^{\alpha_i}$ $(i = 1, 2, \ldots, k)$, мы из $b \vdots a$ получаем требуемое простой ссылкой на теорему 2.

Достаточность доказывается по индукции. Делимость $b \vdots p_1^{\alpha_1}$ мы имеем в числе условий. Предположим, что нами уже установлено, что

$$b \vdots p_1^{\alpha_1} \dots p_l^{\alpha_l} \quad (1 \leqq l < k).$$

Кроме того, в нашем распоряжении имеется делимость $b \vdots p_{l+1}^{\alpha_{l+1}}$. Так как числа $p_1^{\alpha_1} \dots p_l^{\alpha_l}$ и $p_{l+1}^{\alpha_{l+1}}$ по предыдущей теореме взаимно просты, мы можем применить следствие теоремы 11, которое дает нам

$$b \vdots p_1^{\alpha_1} \dots p_l^{\alpha_l} p_{l+1}^{\alpha_{l+1}}.$$

Этим индуктивный переход обоснован.

17. Необходимость. Пусть $a \vdots b$. Из теоремы 13 следует, что каждый простой делитель b является простым делителем a. Таким образом, b имеет вид

$$p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k},$$

где $0 \leqq \beta_1$, $0 \leqq \beta_2$, ..., $0 \leqq \beta_k$. Предположим, что $\beta_1 > \alpha_1$. Так как

$$\frac{a}{b} = \frac{p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}}{p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}} = \frac{p_2^{\alpha_2} \dots p_k^{\alpha_k}}{p_1^{\beta_1 - \alpha_1} p_2^{\beta_2} \dots p_k^{\beta_k}}$$

— целое число, числитель последней дроби должен делиться на знаменатель и тем более на число $p_1^{\beta_1 - \alpha_1}$. Но тогда по теореме 13 на p_1 должно делиться хотя бы одно из чисел p_2, ..., p_k, чего не может быть. Значит, $\beta_1 \leqq \alpha_1$. Так как нумерация простых делителей a для нас безразлична, мы тем самым доказали, что и $\beta_2 \leqq \alpha_2$, ..., $\beta_k \leqq \alpha_k$. Необходимость доказана.

Для доказательства достаточности заметим, что если b имеет указанный вид, то

$$a = b p_1^{\alpha_1 - \beta_1} p_2^{\alpha_2 - \beta_2} \dots p_k^{\alpha_k - \beta_k}.$$

18. Напишем канонические разложения чисел m и t:

$$m = p_1^{\alpha_1} \dots p_n^{\alpha_n}, \quad t = q_1^{\beta_1} \dots q_l^{\beta_l}.$$

Отберем среди простых p_1, ..., p_n те, которые делят t, т. е. содержатся среди q_1, ..., q_l. Пусть для определенности это будут p_1, ..., p_r, равные соответ-

ственно числам $q_1, \ldots, q_r$. Положим тогда

$$m_2 = p_1^{\alpha_1} \ldots p_r^{\alpha_r}, \quad m_1 = p_{r+1}^{\alpha_{r+1}} \ldots p_n^{\alpha_n}.$$

Согласно теореме 15 будет $(m_1, t) = 1$. Кроме того, возьмем натуральное число k, которое было бы не меньше каждого из отношений

$$\frac{\alpha_1}{\beta_1}, \ldots, \frac{\alpha_r}{\beta_r}.$$

Это значит, что $k\beta_i \geqq \alpha_i$ для $i = 1, \ldots, r$, откуда согласно теореме 17 $t^k \vdots m_2$.

19. Необходимость. Пусть

$$a = mq_1 + r_1 \quad (0 \leqq r_1 < m), \qquad (Д.4)$$

$$b = mq_2 + r_2 \quad (0 \leqq r_2 < m). \qquad (Д.5)$$

Ввиду равноостаточности a и b должно быть $r_1 = r_2$. Значит,

$$a - b = m(q_1 - q_2),$$

т. е. $(a - b) \vdots m$.

Достаточность. Пусть $(a - b) \vdots m$. Разделив a и b на m с остатком, мы получим (Д.4) и (Д.5). При этом

$$a - b = m(q_1 - q_2) + r_1 - r_2,$$

т. е.

$$(a - b) - m(q_1 - q_2) = r_1 - r_2.$$

По теореме 6 $(r_1 - r_2) \vdots m$. Но $|r_1 - r_2| < m$. Значит, по теореме 4 $r_1 - r_2 = 0$ или $r_1 = r_2$, а это и требовалось.

20. Из условия на основании теоремы 16 мы имеем

$$\begin{aligned} a_1 &= b_1 + mq_1, \\ a_2 &= b_2 + mq_2, \\ &\ldots\ldots\ldots \\ a_n &= b_n + mq_n. \end{aligned} \qquad (Д.6)$$

Сложив почленно эти равенства, мы после простых преобразований получаем

$$(a_1 + a_2 + \ldots + a_n) - (b_1 + b_2 + \ldots + b_n) = m(q_1 + q_2 + \ldots + q_n),$$

что по теореме 19 и означает равноостаточность сумм.

Сходным образом доказывается равноостаточность произведений. Перемножим почленно все равенства (Д.6):

$$a_1a_2 \ldots a_n = (b_1 + mq_1)(b_2 + mq_2) \ldots (b_n + mq_n).$$

Раскрывая справа скобки, мы получим произведение $b_1b_2 \ldots b_n$ и еще $2^n - 1$ произведений, в каждом из которых имеется хотя бы один из сомножителей, равный m. Это значит, что последнее равенство может быть записано в виде

$$a_1a_2 \ldots a_n = b_1b_2 \ldots b_n + mt,$$

где t — некоторое целое число. Равноостаточность произведений, таким образом, доказана.

21. Необходимость. Если описанный алгорифм является признаком равноостаточности при делении на m, то числа A и b при делении на m должны быть равноостаточными. В частности, это будет так, если $A = t^k + b$. Но это значит, что

$$A - b = t^k \vdots m.$$

Достаточность. В наших обозначениях $A - b = at^k$, т. е. числа A и b равноостаточны при делении на t^k. Если $t^k \vdots m$, то по следствию теоремы 17 они равноостаточны и при делении на m. Поэтому конструируемая алгорифмом в этом случае последовательность A_0, A_1, ... состоит из равноостаточных при делении на m чисел. Следовательно, процесс построения этой последовательности является признаком равноостаточности при делении на m.

22. Необходимость. Если описанный алгорифм действительно является признаком равноостаточности при делении на m, то он, в частности, должен быть применим и к числу $A = t^k + a_0$. Здесь $f(A) = a_0 + 1$, и равноостаточность чисел A и $f(A)$ при делении на m означает $(t^k - 1) \vdots m$.

Достаточность. Пусть $A \geqq t^k$. Тогда из определения функции f следует, что

$$A - f(A) =$$

$$= a_n(t^{kn} - 1) + a_{n-1}(t^{k(n-1)} - 1) + \ldots + a_1(t^k - 1).$$

Здесь каждое слагаемое (см., например, задачу 22д)) делится на $t^k - 1$. Значит, если $(t^k - 1) \vdots m$, то и $(A - f(A)) \vdots m$. Равноостаточность остальных членов

последовательности (3.4), а также ее членов, если она начинается с числа $A < t^k$, вытекает из ее построения.

23. Необходимость. В случае $A = t^k + a_0$ равноостаточность чисел A и $f(A) = a_0 - 1$ при делении на m дает нам $(t^k + 1) \vdots m$.

Достаточность. Мы имеем в нашем случае при $A \geqq t^k$

$$A - f(A) = a_n(t^{kn} \pm 1) + a_{n-1}(t^{k(n-1)} \mp 1) + \ldots$$
$$\ldots + a_1(t^k + 1) \quad (Д.7)$$

(знак «плюс» стоит здесь в члене, соответствующем нечетному коэффициенту при k в показателе, а знак «минус» — в члене, соответствующем четному коэффициенту). Согласно д) и е) задачи 22 при нечетном r выражение $t^{kr} + 1$ делится на $t^k + 1$, а при четном r на $t^k + 1$ делится выражение $t^{kr} - 1$. Значит, если $(t^k + 1) \vdots m$, то на m делится каждый член в (Д.7) справа, а потому и вся разность $A - f(A)$. Тем самым числа A и $f(A)$ оказываются равноостаточными при делении на m. Равноостаточность остальных членов последовательности (3.4), а также членов этой последовательности, если она начинается с числа $A < t^k$, вытекает непосредственно из ее построения.

24. Доказательство ведется индукцией по a. При $a = 1$ имеем

$$a^p - a = 1 - 1 = 0$$

и $0 \vdots p$.

Предположим, что $a^p - a$ делится на p, и докажем, что $(a+1)^p - (a+1)$ также делится на p. Действительно, разлагая $(a+1)^p$ по формуле бинома Ньютона, имеем

$$(a+1)^p - (a+1) =$$
$$= a^p + C_p^1 a^{p-1} + C_p^2 a^{p-2} + \ldots + C_p^{p-1} a + 1 - a - 1 =$$
$$= a^p - a + C_p^1 a^{p-1} + C_p^2 a^{p-2} + \ldots + C_p^{p-1} a. \quad (Д.8)$$

Здесь $a^p - a$ делится на p по предположению. По следствию теоремы 13 C_p^k (при $1 \leqq k \leqq p-1$) также делится на p. Следовательно, на p делится каждое слагаемое правой части соотношения (Д.8), а потому (теорема 6) и вся сумма.

Индуктивный переход обоснован, и вся теорема доказана.

Следствие. *По теореме Ферма*

$$a^p - a = a(a^{p-1} - 1) \vdots p.$$

Если при этом a *не делится на* p, *то по теореме* 13 *на* p *должно делиться* $a^{p-1} - 1$.

25. Пусть

$$m_1 = p_1^{\alpha_1} \dots p_k^{\alpha_k}, \quad m_2 = q_1^{\beta_1} \dots q_l^{\beta_l}.$$

По теореме 15 каждое из чисел $p_1, \dots, p_k$ отлично от каждого из чисел $q_1, \dots, q_l$. Значит, каноническим разложением $m_1 m_2$ будет $p_1^{\alpha_1} \dots p_k^{\alpha_k} q_1^{\beta_1} \dots q_l^{\beta_l}$. Поэтому

$$\varphi(m_1 m_2) = p_1^{\alpha_1 - 1}(p_1 - 1) \dots p_k^{\alpha_k - 1}(p_k - 1) \times \\ \times q_1^{\beta_1 - 1}(q_1 - 1) \dots q_l^{\beta_l - 1}(q_l - 1),$$

т. е.

$$\varphi(m_1 m_2) = \varphi(m_1)\varphi(m_2).$$

26. Докажем сначала индукцией по α, что $a^{p^{\alpha-1}(p-1)} - 1$ делится на p^α. При $\alpha = 1$ доказываемое утверждение является, очевидно, следствием теоремы Ферма, справедливость которого уже была установлена. Таким образом, основание индукции доказано.

Предположим теперь, что

$$(a^{p^{\alpha-1}(p-1)} - 1) \vdots p^\alpha,$$

и рассмотрим выражение $a^{p^\alpha(p-1)} - 1$. Мы должны доказать, что оно делится на $p^{\alpha+1}$. Но

$$a^{p^\alpha(p-1)} - 1 = (a^{p^{\alpha-1}(p-1)})^p - 1.$$

Так как $a^{p^{\alpha-1}(p-1)} - 1$ по предположению делится на p^α, число $a^{p^{\alpha-1}(p-1)}$ имеет вид $Np^\alpha + 1$. Значит,

$$a^{p^\alpha(p-1)} - 1 = (Np^\alpha + 1)^p - 1,$$

т. е. по формуле бинома

$$a^{p^\alpha(p-1)} - 1 = \\ = N^p p^{\alpha p} + C_p^1 N^{p-1} p^{\alpha(p-1)} + \dots + C_p^{p-1} N p^\alpha + 1 - 1.$$

В последней сумме первое слагаемое делится на $p^{\alpha+1}$, так как оно делится на $p^{\alpha p}$ и $\alpha p \geqq \alpha + 1$. В каждое из следующих $p - 1$ слагаемых этой суммы входит p с показателем, не меньшим α, и, кроме того, биномиаль-

ный коэффициент, в силу следствия теоремы 13 делящийся на p. Значит, каждое из этих слагаемых также делится на $p^{\alpha+1}$. Наконец, разность $1-1=0$ может быть отброшена. Поэтому по теореме 6

$$(a^{p^{\alpha}(p-1)}-1) \vdots p^{\alpha+1}.$$

Случай, когда число m имеет только один простой делитель, таким образом, разобран.

Предположим теперь, что теорема Эйлера верна для показателей m_1 и m_2, причем числа m_1 и m_2 взаимно простые, и докажем ее для показателя $m=m_1m_2$. Если потом положить

$$m_1=p_1^{\alpha_1}\dots p_k^{\alpha_k},\quad m_2=p_{k+1}^{\alpha_{k+1}},$$

то мы, очевидно, и получим индуктивный переход, необходимый нам для завершения доказательства теоремы. Итак, доказываем высказанное утверждение.

Пусть числа a и m взаимно просты. Тогда a также взаимно просто с m_1. Значит, и $a^{\varphi(m_2)}$ взаимно просто с m_1. Поэтому, по предположению,

$$(a^{\varphi(m_2)})^{\varphi(m_1)}-1=a^{\varphi(m_1)\varphi(m_2)}-1=a^{\varphi(m_1m_2)}-1=a^{\varphi(m)}-1$$

делится на m_1. Точно так же убеждаемся в том, что $a^{\varphi(m)}-1$ делится и на m_2. А так как числа m_1 и m_2 взаимно простые, $a^{\varphi(m)}-1$ делится и на их произведение, т. е. на m. Теорема Эйлера доказана.

27. Пусть

$$k_1=\varphi(m)q_1+r,$$
$$k_2=\varphi(m)q_2+r.$$

Тогда

$$a^{k_1}=a^{\varphi(m)q_1+r}=(a^{\varphi(m)})^{q_1}a^r.$$

На основании теоремы Эйлера и теоремы 20 число $a^{\varphi(m)q_1}a^r$ равноостаточно при делении на m с числом a^r. Аналогично устанавливается равноостаточность при этом делении чисел a^{k_2} и a^r. Значит, и числа a^{k_1} и a^k при делении на m равноостаточны.

28. Найдем сначала хотя бы одно решение (x', y') этого уравнения. Очевидно, что для этого достаточно найти такое число x', что $(ax'-c) \vdots b$. По теореме Эйлера $(a^{\varphi(b)}-1) \vdots b$. Значит, $(ca^{\varphi(b)}-c) \vdots b$, и в качестве x' можно взять число $ca^{\varphi(b)-1}$.

Пусть теперь (x'', y'') — какое-то другое решение уравнения $ax+by=c$. Покажем, что числа x' и x''

равноостаточны при делении на b. В самом деле, пусть

$$ax' + by' = c,$$
$$ax'' + by'' = c.$$

Вычитая почленно второе равенство из первого, получаем

$$a(x' - x'') - b(y' - x'') = 0,$$

откуда $a(x' - x'') \vdots b$. Так как a и b по условию взаимно просты, по теореме 12 будет $(x' - x'') \vdots b$, и нам остается сослаться на теорему 19.

Таким образом, все искомые значения x находятся среди чисел,

$$x_t = ca^{\varphi(b)-1} + bt.$$

Но $(ax_t - c) \vdots b$, так что, полагая

$$y_t = \frac{-ax_t + c}{b} = c\frac{1 - a^{\varphi(b)}}{b} - at,$$

мы получаем, что все пары чисел x_t и y_t являются решениями нашего уравнения.

29. Ввиду взаимной простоты m и 10, числа $10a+b$ и $(10a + b)10^{\varphi(m)-1}$ по теореме 15 равноделимы на m. Но

$$(10a + b)10^{\varphi(m)-1} = 10^{\varphi(m)}a + 10^{\varphi(m)-1}b,$$

так что по теореме Эйлера и теореме 20 число $10a + b$ равноделимо на m с числом $a + kb$.

РЕШЕНИЯ ЗАДАЧ

1. $0 = a \cdot 0$ при любом a.

2. $a = 1 \cdot a$, значит, $a \vdots 1$.

3. Пусть $1 \vdots a$. Это значит, что $1 = ac$ при некотором целом c. Отсюда следует, что $|a| \leqq 1$. А так как $a \neq 0$, должно быть $a = 1$.

4. Достаточно взять любое $c > 1$ и положить $b = ac$.

5. В качестве такого b можно взять, например, $2a$. Пусть при этом для некоторого c и $2a \vdots c$ и $c \vdots a$. Это значит, что найдутся такие d_1 и d_2, что $2a = d_1 c$ и $c = d_2 a$. Отсюда следует, что $2a = d_1 d_2 a$ или, после сокращения на a,

$$2 = d_1 d_2.$$

Но при целых d_1 и d_2 такое равенство возможно лишь в случае, когда одно из этих чисел равно 1, а другое 2. Если $d_1 = 1$, то $c = 2a = b$; если же $d_2 = 1$, то $c = a$.

6. Доказательства ничем не отличаются от доказательств в случае обычной делимости.

7. Пусть n — некоторое фиксированное число, большее единицы. Положим $a \underset{n}{\vdots} b$, если найдется такое целое c, что $a = bc$ и $c \leqq n$. Справедливость теорем, аналогичных теоремам 1, 3 и 4, проверяется без труда. Однако если мы возьмем $a = nb$ и $b = nc$, то $a \underset{n}{\vdots} b$ и $b \underset{n}{\vdots} c$. В этом случае $a = n^2 c$, а так как $n^2 > n$, делимость $a \underset{n}{\vdots} c$ не имеет места. Точно так же в этом случае не имеет места делимость $(a + a) \underset{n}{\vdots} b$.

8. а) Пусть имеются два минимальных числа a_1 и a_2. В силу дихотомичности либо $a_1 \geqq a_2$, либо $a_2 \geqq a_1$. Если $a_1 \geqq a_2$, то из минимальности a_1 следует, что $a_1 = a_2$. Если же $a_2 \geqq a_1$, то $a_1 = a_2$ следует из минимальности a_2.

б) Пусть a — некоторое число, а b_1 и b_2 — два непосредственно предшествующих ему числа. По дихотомичности должно быть либо $b_1 \geqq b_2$, либо $b_2 \geqq b_1$. Пусть, для определенности, $b_1 \geqq b_2$. Мы имеем $a \geqq b_1 \geqq b_2$, а так как число b_2 непосред-

ственно предшествует числу a, должно быть либо $b_1 = a$, либо $b_1 = b_2$. Но по условию $b_1 \neq a$; значит, $b_1 = b_2$, и требуемая единственность доказана.

в) *Непосредственно следующим* за a числом называется такое b, что $b \geqq a$, $b \neq a$, и из $b \geqq c \geqq a$ следует либо $c = b$, либо $c = a$.

Предположим, что некоторое a не имеет непосредственно следующего за ним числа. Это значит, что для любого $a_n \geqq a$ и отличного от a найдется такое a_{n+1}, отличное как от a_n, так и от a, что $a_n \geqq a_{n+1} \geqq a$. Возьмем теперь произвольное $a_1 \geqq a$ и отличное от a (в силу 2° это сделать можно) и, исходя из него, построим бесконечную последовательность различных чисел

$$a_1 \geqq a_2 \geqq \ldots \geqq a_n \geqq a_{n+1} \geqq \ldots \geqq a.$$

Существование же этой последовательности противоречит 4°. Следовательно, непосредственно следующее число существует. Единственность его устанавливается при помощи дихотомичности подобно тому, как это делалось в а) и б).

9. Остается в силе транзитивность (3°), неограниченность множества чисел (5°), свойство 4° и существование непосредственно предшествующего числа (6°). Дихотомичность заменяется *трихотомичностью* (либо $a > b$, либо $b > a$, либо $a = b$).

Становится неверным свойство рефлексивности (1°), ибо $a > a$ всегда неверно.

Что же касается, наконец, утверждения 2°, то формально оно остается в силе (хотя, быть может, и выглядит несколько парадоксально).

В самом деле, говоря строго, это утверждение в нашем случае формируется так: для любых натуральных чисел a и b из $a > b$ и $b > a$ следует $a = b$.

Предположим, что это высказывание неверно. Тогда найдутся такие натуральные числа a и b, что одновременно будет и $a > b$ и $b > a$, и $a \neq b$, а этого не может быть. Полученное противоречие доказывает истинность нашего утверждения.

10. Пусть множество упорядочено отношением $\leftarrow$, обладающим свойствами 1°—7°. Как уже было установлено, оно обладает минимальным элементом. Обозначим этот элемент через a_0. Из результатов задачи 8 следует, что каждый элемент обладает непосредственно следующим. Обозначим непосредственно следующий за a_0 элемент через a_1, непосредственно следующий за a_1 — через a_2 и т. д. В итоге мы получаем последовательность

$$a_0, a_1, a_2, \ldots, \qquad \text{(Р.1)}$$

в которой $a_{n+1} \leftarrow a_n$ при любом n. По рефлексивности и транзитивности отношения $\leftarrow$ отсюда следует, что $a_i \leftarrow a_j$ тогда и только тогда, когда $i \geqq j$. Нам остается показать, что последовательность (Р.1) охватывает все рассматриваемые нами объекты. Это достигается довольно тонким рассуждением по индукции.

Предположим, что b_0 не принадлежит последовательности (Р.1). Получение этого b_0 будем считать первым шагом нашего индуктивного рассуждения. Пусть n его шагов уже проведены, в результате чего нами получен некоторый элемент b_{n-1}.

Если $b_{n-1} = a_0$, то наш процесс будем считать законченным; если же $b_{n-1} \neq a_0$, то элемент b_{n-1} имеет непосредственно предшествующий, который мы и возьмем в качестве b_n. В результате

мы получаем последовательность различных элементов

$$b_0 \prec b_1 \prec b_2 \prec \ldots \prec b_n \prec \ldots$$

На основании 4° эта последовательность должна иметь последний член. Но по самому принципу построения этой последовательности ее последним членом может быть только a_0. Пусть для определенности $b_n = a_0$.

Нетрудно проверить, что если некоторое a непосредственно предшествует b, то b непосредственно следует за a. Значит, $b_{n-1} = a_1$, $b_{n-2} = a_2$, ..., $b_0 = a_n$.

Последнее означает, что b_0 принадлежит последовательности (Р.1), но это противоречит предположенному. Следовательно, последовательность (Р.1) содержит все рассматриваемые нами объекты.

11. Пусть a — некоторое число. Всякую последовательность различных чисел $a_0 = a$, a_1, a_2, ..., a_n, для которых

$$a_0 \prec a_1 \prec a_2 \prec \ldots \prec a_n, \qquad (Р.2)$$

где a_n минимально в смысле упорядочения $\prec$, назовем *цепью предшественников* a_0. Число n называется *длиной* этой цепи.

Покажем сначала, что при тех условиях, которые мы наложили на упорядочение $\prec$, каждое конкретное число не может иметь сколь угодно длинных цепей предшественников.

В самом деле, пусть a — некоторое число, а b_1, b_2, ..., b_k — непосредственно предшествующие ему числа.

Если a_1 не предшествует a_0 непосредственно, мы можем на основании 9° вставить в цепь (Р.2) некоторое непосредственно предшествующее a число. Поэтому если имеются сколь угодно длинные цепи предшественников a, должны найтись и такие его сколь угодно длинные цепи предшественников, которые начинаются с чисел, непосредственно предшествующих a. Будем далее рассматривать только такие цепи.

Каждая цепь предшественников a ровно на единицу длиннее некоторой цепи предшественников одного из непосредственно предшествующих ему чисел. Если бы каждое из них имело цепи предшественников ограниченной длины, то само a не могло бы иметь сколь угодно длинных цепей предшественников.

Значит, при нашем предположении хотя бы одно из чисел, непосредственно предшествующих a_0, имеет сколь угодно длинные цепи предшественников. Обозначим это число через a_1 и повторим в применении к нему все только что проведенные рассуждения. Это даст нам некоторое число a_2, непосредственно предшествующее a_1 и имеющее сколь угодно длинные цепи предшественников. Повторяя этот процесс, мы приходим к последовательности

$$a_0 \prec a_1 \prec a_2 \prec \ldots,$$

которая в силу 4° должна рано или поздно оборваться. Это значит, что последовательность будет иметь такой член, к которому наши рассуждения уже будут неприменимы. Но применимость рассуждений к каждому последующему члену последовательности нами уже была установлена. Полученное противоречие показывает, что ни одно число не имеет сколь угодно длинных цепей предшественников.

Следовательно, для каждого числа a среди его цепей предшественников можно выбрать самую длинную. Обозначим ее

длину через $n(a)$. Если b непосредственно предшествует a, то, очевидно, $n(b) = n(a) - 1$, а для всех минимальных a $n(a) = 0$.

Пусть, наконец, $A(a)$ — высказывание, зависящее от a. Обозначим через $B(n)$ высказывание «$A(a)$ верно для всех чисел a, для которых $n(a) = n$». Тогда, как легко видеть, формулировка принципа индукции в новой форме для утверждений $A(a)$ совпадает с формулировкой этого принципа в старой форме для утверждений $B(n)$.

12. Каковы бы ни были четные числа a и b, существуют такие четные числа q и r, что

$$a = bq + r \qquad (0 \leqq r < 2b).$$

Такие числа q и r единственны.

Доказательство. Разделим a на $2b$ с остатком обычным образом:

$$a = 2bq + r \qquad (0 \leqq r < 2b). \qquad \text{(Р.3)}$$

При этом числа q и r определяются однозначно. Из четности a и $2bq$ следует четность их разности, т. е. числа r. Нам остается, положив $2q = q'$, переписать (Р.3) в виде

$$a = q'b + r \qquad (0 \leqq r < 2b)$$

и заметить, что оба числа q' и r четные и определяются единственным образом.

13. Пусть p — наименьший простой делитель числа a. Отсюда следует, что $a = pb$. Всякий простой делитель q числа b является вместе с тем и делителем a. Поэтому $q \geqq p$, значит, и $b \geqq p$, так что $a \geqq p^2$ и, наконец, $p \leqq \sqrt{a}$.

14. Пусть $p_1, p_2, \ldots, p_k$ — полный список всех простых чисел, входящих хотя бы в одно из канонических разложений a и b. Положим

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k},$$

$$b = p_1^{\beta_1} p_2^{\beta_2} \ldots p_k^{\beta_k}.$$

(Если a не делится на p_i, то $\alpha_i = 0$; если b не делится на p_i, то $\beta_i = 0$.) Пусть γ_i — наибольшее из чисел α_i и β_i для $i = 1, 2, \ldots, k$, а δ_i — наименьшее из них.

Тогда на основании теоремы 17 наибольший общий делитель a и b есть $p_1^{\delta_1} p_2^{\delta_2} \ldots p_k^{\delta_k}$, а их наименьшее общее кратное есть $p_1^{\gamma_1} p_2^{\gamma_2} \ldots p_k^{\gamma_k}$.

15. Как следует из теоремы 17, каждый делитель числа a с каноническим разложением $p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ должен иметь вид $p_1^{\beta_1} \ldots p_k^{\beta_k}$, где β_1 принимает $\alpha_1 + 1$ значений: 0, 1, 2, ..., α_1; β_2 принимает $\alpha_2 + 1$ значений и т. д. Так как любые комбинации этих значений возможны и дают нам все делители a, причем

каждый по одному разу (если бы какой-нибудь делитель повторился несколько раз, то это означало бы наличие у него нескольких канонических разложений), число делителей a равно

$$(\alpha_1 + 1)(\alpha_2 + 1) \ldots (\alpha_k + 1). \qquad \text{(Р.4)}$$

16. Пусть каноническое разложение a есть $p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$. Очевидно, можно положить $p_1 = 2$, $\alpha_1 \geqq 2$ и $p_2 = 3$, $\alpha_2 \geqq 1$. Далее, согласно (Р.4) имеем

$$(\alpha_1 + 1)(\alpha_2 + 1) \ldots (\alpha_k + 1) = 14.$$

Отсюда $k = 2$, $\alpha_1 + 1 = 7$ и $\alpha_2 + 1 = 2$. Таким образом, $a = 2^6 \cdot 3 = 192$.

Здесь $\alpha_1 + 1 = 2$ и $\alpha_2 + 1 = 7$ быть не может, так как тогда будет $a = 2 \cdot 3^6$ и a на 4 не делится.

17. Мы имеем

$$\tau(a^2) = \tau\left(p_1^{2\alpha_1} p_2^{2\alpha_2}\right) = (2\alpha_1 + 1)(2\alpha_2 + 1) = 81,$$

так что $(2\alpha_1 + 1)(2\alpha_2 + 1)$ есть разложение числа 81 на два множителя. Так как нумерация простых делителей a зависит от нас, ограничимся рассмотрением следующих возможностей:

$$2\alpha_1 + 1 = 1, \quad 2\alpha_2 + 1 = 81;$$
$$2\alpha_1 + 1 = 3, \quad 2\alpha_2 + 1 = 27;$$
$$2\alpha_1 + 1 = 9, \quad 2\alpha_2 + 1 = 9.$$

В первом из этих случаев $\alpha_1 = 0$, что противоречит предположенной положительности числа α_1. Оставшиеся случаи дают нам

$$\alpha_1 = 1, \quad \alpha_2 = 13;$$
$$\alpha_1 = 4, \quad \alpha_2 = 4.$$

Значит, либо

$$\tau(a^3) = \tau\left(p_1^{3\alpha_1} p_2^{3\alpha_2}\right) = \tau\left(p_1^3 p_2^{39}\right) = (3 + 1)(39 + 1) = 160,$$

либо

$$\tau(a^3) = \tau\left(p_1^{3\alpha_1} p_2^{3\alpha_2}\right) = \tau\left(p_1^{12} p_2^{12}\right) = 13 \cdot 13 = 169.$$

18. Пусть $p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ — каноническое разложение числа a. Условие задачи дает нам

$$p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k} = 2(\alpha_1 + 1)(\alpha_2 + 1) \ldots (\alpha_k + 1),$$

или

$$\frac{p_1^{\alpha_1}}{\alpha_1 + 1} \frac{p_2^{\alpha_2}}{\alpha_2 + 1} \ldots \frac{p_k^{\alpha_k}}{\alpha_k + 1} = 2. \qquad \text{(Р.5)}$$

Заметим, что

$$\frac{2^1}{1+1} = 1 < \frac{2^2}{2+1} = \frac{4}{3} < \frac{2^3}{3+1} = 2 < \frac{2^\alpha}{\alpha+1} \qquad (\alpha \geqq 4),$$

$$1 < \frac{3^1}{1+1} < 2 < \frac{3^\alpha}{\alpha+1} \qquad (\alpha \geqq 2),$$

$$2 < \frac{p^\alpha}{\alpha+1} \qquad (p \geqq 5,\ \alpha \geqq 1).$$

Поэтому в (Р.5) слева каждая дробь не меньше единицы и, следовательно, ни одна из дробей не может быть больше чем 2. Значит, в левой части (Р.5) могут стоять лишь дроби из следующего набора:

$$\frac{2^1}{1+1},\ \frac{2^2}{2+1},\ \frac{2^3}{3+1},\ \frac{3^1}{1+1},$$

причем их произведение есть 2. Но это может быть лишь в двух случаях: когда в (Р.5) слева стоит только одна дробь $\frac{2^3}{3+1}$ или когда там стоят две дроби $\frac{2^2}{2+1}$ и $\frac{3^1}{1+1}$. Этим двум случаям соответствуют два ответа задачи: 8 и 12.

19. Напишем каноническое разложение числа a:

$$a = p_1^{\alpha_1} \dots p_k^{\alpha_k}.$$

Тогда

$$a^2 = p_1^{2\alpha_1} \dots p_k^{2\alpha_k},$$

и согласно (Р.4) (задача 15)

$$\frac{\tau(a^2)}{\tau(a)} = \frac{(2\alpha_1+1)\dots(2\alpha_k+1)}{(\alpha_1+1)\dots(\alpha_k+1)}.$$

Легко видеть, что каждая дробь $(2\alpha_i+1)/(\alpha_i+1)$ с ростом α_i возрастает (приближаясь к 2), так что наименьшее значение этой дроби будет достигаться при $\alpha_i = 1$ и будет равно 3/2. Это значит, что

$$\frac{\tau(a^2)}{\tau(a)} \geqq \left(\frac{3}{2}\right)^k.$$

Ясно, что при достаточно большом k будет $(3/2)^k > K$. Для этого достаточно взять

$$k > \frac{\lg K}{\lg (3/2)}.$$

Например, при $K = 100$ достаточно взять $k > 2/0{,}18 = 11{,}1$; так как число k должно быть целым, можно взять $k = 12$.

20. Аналоги теорем 11—14 для четной делимости неверны. В самом деле, числа 30 и 42 четно простые. Их наименьшее четное кратное есть 420, а произведение равно 1260.

Далее, $60 = 6 \cdot 10$ четно делится на четно простое число 30; 6 и 30 четно взаимно просты, а 10 четно на 30 не делится.

Наконец, $60 = 6 \cdot 10 = 30 \cdot 2$ — два различных разложения числа 60 на четно простые множители.

21. а) 116 при делении на 8 равноостаточно с 4, а 17 — с 1. Значит, A равноостаточно с $5^{21} = (5^2)^{10} \cdot 5$. Но $5^2 = 25$ при делении на 8 равноостаточно с единицей. Следовательно, A при делении на 8 дает в остатке 5.

б) 14 при делении на 17 равноостаточно с -3. Поэтому A равноостаточно с $(-3)^{256} = 3^{256} = (3^3)^{85} \cdot 3$. Но 3^3 мы можем заменить на 10: $10^{85} \cdot 3 = (10^2)^{42} \cdot 30$.

Далее, 10^2 при делении на 17 равноостаточно с числом -2, а 2^4 с -1. Значит, A равноостаточно с $(-2)^{42}\cdot 30 = 2^{42}\cdot 30 = (2^4)^{10}\cdot 4\cdot 30 = (-1)^{10}\cdot 4\cdot 30 = 120$. Последнее же число при делении на 17 дает в остатке 1.

22. а) Пусть n_1 — остаток от деления n на 6. Тогда n_1 может принимать значения 0, 1, 2, 3, 4 и 5, а $n_1^3 + 11n_1$ при делении на 6 равноостаточно с $n^3 + 11n$. Значит, нам следует испытывать делимость на 6 чисел 0, 12, 30, 60, 108 и 180. Но все эти числа на 6 делятся.

Для получения того же результата можно воспользоваться и более частными соображениями. Число $n^3 + 11n$ равноостаточно при делении на 6 с числом $n^3 + 11n - 12n = n^3 - n = (n-1)n(n+1)$. Но из трех последовательных целых чисел $n-1$, n и $n+1$ хотя бы одно четное (т. е. делится на 2) и ровно одно делится на 3. Значит (согласно следствию теоремы 11), произведение этих трех чисел делится на 6. Кстати, можно заметить, что

$$\frac{1}{6}(n-1)\,n\,(n+1) = C_{n+1}^3.$$

б) При $n \geqq 2$ мы имеем (пользуясь формулой бинома)

$$4^n + 15n - 1 = (3+1)^n + 15n - 1 =$$
$$= 3^n - 3^{n-1}C_n^1 + \ldots + 3^2 C_n^{n-2} + 3C_n^{n-1} + 1 + 15n - 1 =$$
$$= 9\left(3^{n-2} + 3^{n-3}C_n^1 + \ldots + C_n^{n-2}\right) + 18n,$$

и оба слагаемых, очевидно, делятся на 9.

При $n = 1$ наше выражение равно $4^1 + 15\cdot 1 - 1 = 18$.

в) Доказательство ведется по индукции.

При $n = 0$

$$10^{3^0} - 1 = 10^1 - 1 = 9, \quad 3^{0+2} = 9.$$

Пусть теперь делимость

$$\left(10^{3^n} - 1\right) \vdots\ 3^{n+2}$$

имеет место. Тогда

$$10^{3^{n+1}} - 1 = \left(10^{3^n}\right)^3 - 1^3 = \left(10^{3^n} - 1\right)\left(10^{2\cdot 3^n} + 10^{3^n} + 1\right).$$

Первый сомножитель справа делится на 3^{n+2} по индуктивному предположению. Во втором же сомно-

жителе мы можем заменить десятки на равноостаточные им при делении на 3 единицы; полученное число 3 показывает, что второй сомножитель делится на 3. Следовательно, все произведение делится на $3^{n+3} = 3^{(n+1)+2}$, что и требовалось.

г) При делении на $a^2 - a + 1$, очевидно, a^2 равноостаточно с $a - 1$. Значит, $a^{2n+1} + (a-1)^{n+2}$ равноостаточно с

$$a^{2n+1} + (a^2)^{n+2} = a^{2n+1} + a^{2n+4} = a^{2n+1}(1 + a^3) = a^{2n+1}(1 + a)(1 - a + a^2),$$

что и требовалось.

д) $(n^k - 1) = (n-1)(n^{k-1} + n^{k-2} + \ldots + n + 1)$.

е) $(n^{2l+1} + 1) = (n+1)(n^{2l} - n^{2l-1} + \ldots - n + 1)$.

23. Пусть $\sim$ — эквивалентное отношение на множестве чисел. Возьмем произвольное число a и рассмотрим все числа, эквивалентные a. Все они ввиду транзитивности отношения $\sim$ эквивалентны между собой. Обозначим через K класс всех этих чисел.

Рассмотрим теперь произвольное число b, не принадлежащее K. Если бы было $b \sim c$, где c — некоторое число из K, то было бы и $b \sim a$, чего, однако, не может быть по выбору b. Значит, ни одно из чисел, лежащих вне K, не эквивалентно ни одному из чисел K. Следовательно, K есть класс эквивалентности, содержащий a.

Так как число a было нами взято совершенно произвольно, проведенные рассуждения показывают, что каждое число принадлежит некоторому классу эквивалентности. Это и требовалось.

24. Очевидно, среди чисел 0, 1, ..., m найдутся два, принадлежащие одному классу. Пусть этими числами будут k и l: $k \sim l$. Таких пар чисел из одного класса может оказаться, вообще говоря, и несколько. Выберем ту из них, для которой величина $|k - l|$ будет наибольшей. Поскольку $-l \sim -l$, мы по условию получаем

$$k - l \sim l - l = 0.$$

Далее, находим, что и при любом целом n

$$n(k - l) \sim 0.$$

Наконец, при любом r

$$n(k - l) + r \sim r,$$

т. е. из $a \equiv b \pmod{k - l}$ следует $a \sim b$. Таким образом, классы отношения $\sim$ содержат целиком классы вычетов по модулю m,

Для того чтобы классов $\sim$-эквивалентности было m, необходимо, чтобы каждый класс $\sim$-эквивалентности содержал не более одного класса вычетов и чтобы $k - l = m$.

25. а) Обе части сравнения и модуль можно разделить на одно и то же число (разумеется, отличное от нуля).

В самом деле,

$$ad \equiv bd \pmod{md}$$

означает, что

$$ad - bd = (a - b)\, d \vdots md,$$

т. е. $(a - b) \vdots m$, откуда $a \equiv b \pmod m$.

б) Обе части сравнения можно разделить на число, взаимно простое с модулем.

Действительно, если d и m взаимно просты, то из

$$ad \equiv bd \pmod m,$$

т. е. из $(a - b)d \vdots m$, следует на основании теоремы 12, что $(a - b) \vdots m$, что и требовалось.

26. Предположим, что

$$1 \leqq k < l \leqq p - 1, \qquad ka \equiv la \pmod p.$$

Это значит, что $(l - k)\, a \vdots p$. Поскольку a не делится на p, должно быть $(l - k) \vdots p$. Но и этого не может быть, так как $0 < l - k < p$.

27. Необходимость. Пусть число p простое. Возьмем $0 < q < p$. По предыдущему среди чисел q, $2q$, ..., $(p - 1)q$ найдется ровно одно, дающее при делении на p в остатке единицу. Пусть этим числом будет $\bar{q}q$:

$$\bar{q}q \equiv 1 \pmod p. \qquad \text{(Р.6)}$$

С другой стороны, среди чисел $\bar{q}$, $2\bar{q}$, ..., $(p - 1)\bar{q}$ также может быть лишь одно, дающее при делении на p в остатке единицу. Это, как уже установлено, число $q\bar{q}$.

Выясним, в каких случаях $q = \bar{q}$. Во всех таких случаях сравнение (Р.6) переписывается так:

$$q^2 \equiv 1 \pmod p,$$

или, что то же самое,

$$q^2 - 1 \equiv 0 \pmod p.$$

Это значит, что

$$q^2 - 1 = (q + 1)(q - 1) \vdots p.$$

Ввиду того, что число p простое, по теореме 13 должно быть либо $(q + 1) \vdots p$, либо $(q - 1) \vdots p$. Так как число q заключено между нулем и p, первый из этих случаев возможен лишь при $q = p - 1$, а второй — при $q = 1$. Таким образом, при $p = 2$ и $p = 3$ всегда $q = \bar{q}$, при $p \geqq 5$ — лишь в случаях $q = 1$ и $q = p - 1$.

Следовательно, при $p \geqq 5$ все оставшиеся числа 2, ..., $p - 2$ можно объединить в такие $(p - 3)/2$ пары, что произведение чисел, составляющих каждую из пар, при делении на p дает в остатке 1. Выпишем сравнения вида (Р.6) для всех таких пар, добавив в этот список сравнение

$$p - 1 \equiv p - 1 \pmod p,$$

и перемножим все $(p - 1)/2$ полученных сравнений почленно.

В результате такого умножения мы получим слева произведение всех чисел от 2 до $p - 1$, а справа $p - 1$:

$$2 \cdot 3 \cdot \ldots \cdot (p - 1) \equiv p - 1 \pmod p,$$

или

$$1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p - 1) + 1 \equiv 0 \pmod p.$$

Последнее сравнение означает, что

$$(1 \cdot 2 \cdot \ldots \cdot (p-1) + 1) \vdots p,$$

а это и требовалось.

Остается проверить случаи $p = 2$ и $p = 3$. Но для них, очевидно, $(1 + 1) \vdots 2$ и $(2 + 1) \vdots 3$.

Достаточность. Если число p не простое, то оно может быть разложено в произведение двух меньших множителей: $p = p_1 p_2$.

Если $p_1 \neq p_2$, то и p_1 и p_2 входят сомножителями в произведение $1 \cdot 2 \cdot \ldots \cdot (p-1)$, которые тем самым делятся на $p_1 p_2$, т. е. на p. Пусть теперь $p_1 = p_2 = q$. Тогда $p = q^2$ (т. е. p есть квадрат простого числа). Если $q > 2$, то $p > 2q$, и в произведение $1 \cdot 2 \cdot \ldots \cdot (p-1)$ входят множителями q и $2q$, так что в этом случае оно делится на q^2, т. е. на p. В обоих случаях $1 \cdot 2 \cdot \ldots \cdot (p-1) + 1$ на p делиться не может. Наконец, если $p = 4$, то $1 \cdot 2 \cdot 3 - 1 = 5$ и на 4 не делится.

28. Теорема. *Пусть* $m = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ *— каноническое разложение* m. *Тогда, для того чтобы числа* A *и* B *были равноостаточными при делении на* m, *необходимо и достаточно, чтобы они были равноостаточными при делении на* $p_1^{\alpha_1}$, *на* $p_1^{\alpha_2}$, ..., *на* $p_k^{\alpha_k}$.

Доказательство. Необходимость. Равноостаточность A и B при делении на m означает $(A - B) \vdots m$. Тем более $(A - B) \vdots p_i^{\alpha_i}$ $(i = 1, \ldots, k)$, и числа A и B оказываются равноостаточными при делении на все $p_i^{\alpha_i}$.

Достаточность. Пусть числа A и B при делении на каждое $p_i^{\alpha_i}$ равноостаточны. Обозначим через r_i остаток от деления A и B на $p_i^{\alpha_i}$ $(i = 1, 2, \ldots, k)$. Это значит, что

$$A \equiv r_i \left(\mathrm{mod}\, p_i^{\alpha_i}\right). \tag{Р.7}$$

Положим, далее,

$$\frac{m}{p_i^{\alpha_i}} = m_i, \quad i = 1, \ldots, k,$$

и умножим в сравнении (Р.7) обе части и модуль на m_i:

$$Am_i \equiv m_i r_i \,(\mathrm{mod}\, m).$$

Сложив все такие сравнения почленно, получим

$$A(m_1 + m_2 + \ldots + m_k) = m_1 r_1 + m_2 r_2 + \ldots + m_k r_k \,(\mathrm{mod}\, m). \tag{Р.8}$$

Ввиду равноостаточности A и B при делении на $p_1^{\alpha_1}$, $p_2^{\alpha_2}$, ..., $p_k^{\alpha_k}$ получаем также

$$B(m_1 + m_2 + \ldots + m_k) \equiv m_1 r_1 + m_2 r_2 + \ldots + m_k r_k \,(\mathrm{mod}\, m). \tag{Р.9}$$

Вычтя почленно сравнение (Р.9) из (Р.8), имеем

$$(A - B)(m_1 + m_2 + \ldots + m_k) \equiv 0 \pmod{m},$$

т. е. $(A - B)(m_1 + m_2 + \ldots + m_k) \vdots m$.

Но сумма $m_1 + m_2 + \ldots + m_k$ взаимно проста с m. В самом деле, если бы она имела с m некоторый общий простой делитель p, то он входил бы в каноническое разложение m, т. е имел бы вид p_i. Но тогда на него делилась бы как вся сумма, так и каждое слагаемое, кроме одного, m_i, а этого быть не может.

Теперь мы можем применить теорему 12, которая даст, что $(A - B) \vdots m$, т. е. числа A и B при делении на m равноостаточны.

29. а) Выпишем систематически все равенства, описывающие деления с остатком, которые составляют применение алгорифма Евклида к числам a и b:

$$\begin{aligned} a &= bq_0 + r_1, \\ b &= r_1q_1 + r_2, \\ r_1 &= r_2q_2 + r_3, \\ &\cdots\cdots\cdots\cdots \\ r_{n-2} &= r_{n-1}q_{n-1} + r_n, \\ r_{n-1} &= r_nq_n. \end{aligned} \qquad \text{(Р.10)}$$

Мы имеем $r_{n-1} \vdots r_n$. Вместе с $r_{n-2} = r_{n-1}q_{n-1} + r_n$ это дает нам $r_{n-2} \vdots r_n$. Продвигаясь аналогичным образом вверх по системе равенств (Р.10), получаем, наконец, что $a \vdots r_n$ и $b \vdots r_n$. Значит, r_n есть общий делитель a и b.

Пусть d — любой общий делитель a и b. Вместе с $a = bq_0 + r_1$ это дает нам $r_1 \vdots d$. Продвигаясь по системе равенств (Р.10) вниз, мы будем последовательно получать, что $r_2 \vdots d$, $r_3 \vdots d$, ..., $r_n \vdots d$. Значит, r_n делится на любой общий делитель a и b, являясь тем самым наибольшим общим делителем этих чисел.

б) Доказательство ведется по индукции. Полагая $A_0 = 0$, $B_0 = 1$, $A_1 = 1$, $B_1 = -q_0$, мы имеем $r_0 = b = aA_0 + bB_0$ и $r_1 = aA_1 + bB_1$.

Пусть теперь

$$\begin{aligned} r_{k-1} &= A_{k-1}a + B_{k-1}b, \\ r_k &= A_ka + B_kb. \end{aligned}$$

Но тогда

$$r_{k+1} = r_{k-1} - r_kq_{k+1} = (A_{k-1} - q_{k+1}A_k)a + (B_{k-1} - q_{k+1}B_k)b,$$

и нам остается положить

$$\begin{aligned} A_{k-1} - q_{k+1}A_k &= A_{k+1}, \\ B_{k-1} - q_{k+1}B_k &= B_{k+1}. \end{aligned}$$

Числа A_n и B_n окажутся искомыми A и B.

30. Если b и c взаимно просты, то по предыдущему можно найти такие целые B и C, что

$$bB + cC = 1,$$

или, после умножения на a,

$$abB + acC = a;$$

$ab \vdots c$ по условию; $ac \vdots c$ очевидным образом; значит, и $a \vdots c$;

31. Ограничимся рассмотрением признака равноостаточности при делении на 8.

Пусть произвольное натуральное A представлено в виде $1000a + b$, где $0 \leqq b < 1000$ (т. е. b — трехзначное число, которым оканчивается A), и

$$f(A) = \begin{cases} b, & \text{если } A \geqq 1000, \\ \text{остатку от деления } A \text{ на } 8, & \text{если } 8 \leqq A < 1000, \\ \text{не определено,} & \text{если } A < 8. \end{cases}$$

Проверка того, что процесс построения последовательности A, $f(A)$, $f(f(A))$ (здесь $f(f(A)) < 8$) действительно является признаком равноостаточности, осуществляется стандартно.

32. Ограничимся рассмотрением признака равноостаточности при делении на 18 в двенадцатеричной системе счисления.

Пусть A представлено в виде $144a + b$, где $0 \leqq b < 144$ (т. е. b — двузначное в двенадцатеричной системе счисления число, которым оканчивается записанное в этой системе число A), и

$$f(A) = \begin{cases} b, & \text{если } A \geqq 144, \\ \text{остатку от деления } A \text{ на } 18, & \text{если } 18 \leqq A < 144, \\ \text{не определено,} & \text{если } A < 18. \end{cases}$$

33. Для тех m, у которых каноническое разложение имеет вид $2^{\alpha} \cdot 5^{\beta}$.

34. Условия а) и б) выполняются автоматически. Поскольку при делении на 3 числа 10 и 1 равноостаточны, равноостаточными же должны быть и числа A и $f(A)$. Наконец, то, что $f(A) < A$ при $A \geqq 3$, устанавливается простым подсчетом.

35. а) $f(858\,773) = 38$; $f(38) = 11$; $f(11) = 2$.

б) $f(A) = 4444 \cdot 4 = 17\,776$; $f(17\,776) = 28$; $f(28) = 10$; $f(10) = 1$.

36. Признак равноостаточности при делении на 9 аналогичен рассмотренному признаку равноостаточности при делении на 3.

Для получения признака равноостаточности при делении на 11 представим число A в виде

$$10^{2n}a_n + 10^{2n-2}a_{n-1} + \ldots + 10^2a_1 + a_0,$$

где $0 \leqq a_i < 100$. Очевидно, такое представление соответствует разбиению числа на двузначные «грани» (справа налево). Пусть

$$f(A) = \begin{cases} a_0 + a_1 + \ldots + a_n, & \text{если } A \geqq 100, \\ \text{остатку от деления } A \text{ на } 11, & \text{если } 11 \leqq A < 100, \\ \text{не определено,} & \text{если } A < 11. \end{cases}$$

Нам остается указать, что числа A и $f(A)$ действительно равноостаточны при делении на 11 и, кроме того, $f(A) < A$.

Другой признак равноостаточности при делении на 11 получается на основе обычной десятичной записи числа A,

$$A = 10^n a_n + 10^{n-1}a_{n-1} + \ldots + 10a_1 + a_0,$$

и использования того, что 10 при делении на 11 равноостаточно с -1, а 100 — с 1. Поэтому A равноостаточно с числом $a_0 - a_1 + a_2 - a_3 + \ldots \pm a_n$, и формулировка соответствующего признака равноостаточности не составляет труда.

Наконец, можно, разбивая число A на трехзначные «грани», представить его в виде

$$10^{3n}a_n + 10^{3n-3}a_{n-1} + \ldots + 10^3a_1 + a_0$$

($0 \leqq a_i < 1000$). Тогда A при делении на 37 равноостаточно с суммой $a_0 + a_1 + \ldots + a_n$, а при делении на 7, 11 и 13 — со знакопеременной суммой $a_0 - a_1 + a_2 - \ldots \pm a_n$.

37. Для примера рассмотрим признак равноостаточности на 8 в троичной системе счисления. Представим для этого произвольное A в виде

$$a_n \cdot 3^{2n} + a_{n-1} \cdot 3^{2(n-1)} + \ldots + a_1 \cdot 3^2 + a_0, \text{ где } 0 \leqq a_i < 9.$$

Здесь a_i суть двузначные грани, на которые разбивается число A, считая справа налево. Нам остается

положить

$$f(A)=\begin{cases} a_0+a_1+\ldots+a_n, & \text{если } A\geqq 9,\\ 0, & \text{если } A=8,\\ \text{не определено}, & \text{если } A<8, \end{cases}$$

и провести стандартные рассуждения.

38. В шестеричной системе счисления: 5 ($k=1$), 7 ($k=2$), 43 ($k=3$);

В семеричной системе счисления: 2, 3, 6 ($k=1$), 4, 6, 12, 16, 24 ($k=2$), 171 ($k=3$);

В девятеричной системе счисления: 2, 4, 8 ($k=1$), 5, 10, 20, 40 ($k=2$), 7, 13, 14, 26 и т. д. ($k=3$);

В тринадцатеричной системе счисления: 2, 3, 4, 6 ($k=1$), 7, 14, 21 и т. д. ($k=2$).

39. В троичной системе счисления: 2, 4 ($k=1$), 8, 12, 24 ($k=2$), 13, 26 ($k=3$), 41 ($k=4$);

В пятеричной системе счисления: 2, 3, 6 ($k=1$), 8, 12, 24 ($k=2$), 31 ($k=3$);

В восьмеричной системе счисления 3, 9 ($k=1$), 5, 13 ($k=2$);

В десятичной системе счисления: 11 ($k=1$), 101 ($k=2$), 7, 11, 13 ($k=3$).

40. Если числа a и b равноостаточны, то $(a-b) \vdots m$. Поэтому в силу теоремы 6 числа a и b делятся или не делятся на m одновременно.

Числа 4 и 5 равноделимы, но не равноостаточны при делении на 3.

41. Пусть из равноделимости на m следует равноостаточность при делении на m. Это значит, что все не делящиеся на m числа имеют при делении на m один и тот же остаток. Значит, этот остаток должен быть равен единице, так что $m=2$.

42. Отношение равноделимости на m, очевидно, является рефлексивным (всякое число равноделимо на m с самим собой), симметричным (если a равноделимо с b, то и b равноделимо с a) и транзитивным (если a равноделимо с b, а b равноделимо с c, то и a равноделимо с c).

Следовательно, это и есть отношение эквивалентности. При этом в один класс попадают все числа, делящиеся на m, а в другой — все не делящиеся на m.

43. Нетрудно проверить, что при $m>2$ равноделимость сумм не следует из равноделимости слагаемых.

Для того чтобы равноделимость произведений вытекала из равноделимости их сомножителей, необходимо и достаточно, чтобы число m было простым.

В самом деле, если одно из произведений делится на простое p, то по теореме 13 на это p должен делиться хотя бы один из сомножителей этого произведения. Но тогда на p делится равноделимый ему сомножитель другого произведения, а потому и все произведение. Если же одно произведение на p не делится, то и другое на p делиться не может (ибо в противном случае на основании только что установленного на p делилось бы и первое произведение).

Наоборот, если число p составное, то произведения равноделимых сомножителей могут уже равноделимыми не быть. Достаточно положить $p = p_1 p_2$ ($p_1 \neq 1$, $p_2 \neq 1$). Тогда числа 1 и p_1, а также числа 1 и p_2 равноделимы на p, а произведения $1 \cdot 1$ и $p_1 \cdot p_2$, очевидно, нет.

44. Непосредственное следствие задачи 36.

45. Выполнение условий а) и б) очевидно.

Если, далее, $a - 2b \geqq 0$, то, очевидно, $f_3(A) < A$. Если же $a - 2b < 0$, то это неравенство может и нарушиться. При этом наибольшее значение модуля $|a - 2b|$ достигается при $a = 0$ и $b = 9$ и равно 18. Следовательно, при $A \geqq 19$ должно быть $f_3(A) < A$. Справедливость этого неравенства при меньших значениях обеспечивается определением функции f.

Наконец, $10a + b$ равноделимо на 7 с $50a + 5b$ (ибо числа 5 и 7 взаимно простые) и тем самым с $50a + 5b - 7(7a + b) = a - 2b$.

46. Число 15 при делении на 7 дает в остатке 1, а $1 - 2 \cdot 5 = -9$ дает в остатке 5.

47. Условие в) $f_4(A) < A$ означает $a + 4b < 10a + b$, т. е. $3b < 9a$. Поэтому при $a \geqq 4$ нужное условие выполняется.

Условие г) очевидно, $10a + b$ при делении на 13 равноделимо с $40a + 4b$, а последнее число равноостаточно с $a + 4b$.

48. Признак делимости утратит результативность, так как $f_4(39) = 39$.

49. Пусть нам нужно построить признак делимости на некоторое m. Постараемся подобрать такое s, взаимно простое с m и по возможности небольшое, что $(10s + 1) \vdots m$ (так было в случае $m = 7$;

s оказалось равным 3) или же $(10s-1) \vdots m$ (например, при $m=13$, $s=4$).

В первом из этих случаев $A=10a+b$ равноделимо на m с

$$10as+bs=(10s+1)a-a+bs,$$

т. е. с $a-bs$, а во втором — с

$$(10s-1)a+a+bs,$$

т. е. с $a+bs$.

В связи со сказанным число $10a+b$

при делении на 17 равноделимо с $a-5b$,
при делении на 19 равноделимо с $a+2b$,
при делении на 23 равноделимо с $a+7b$,
при делении на 29 равноделимо с $a+3b$,
при делении на 31 равноделимо с $a-3b$

и вообще

при делении на $10k \pm 1$ равноделимо с $a \mp kb$.

Завершение точных формулировок этих признаков делимости предоставляется читателю.

50. а) Так как 100 при делении на 49 равноостаточно с 2, всякое число вида

$$10^{2n}a_n+10^{2n-2}a_{n-1}+\ldots+10^2a_1+a_0 \qquad (0 \leqq a_i < 100)$$

при делении на 49 равноостаточно с

$$2^na_n+2^{n-1}a_{n-1}+\ldots+2a_1+a_0.$$

б) $10a+b$ при делении на 49 равноделимо с $a+5b$.

51. Очевидно, при $A \geqq 6$ должно быть $f(A)<A$.

52. а) В семеричной системе счисления представление A в виде $7a+b$ дает, что при делении на 5 число A равноделимо с $a+3b$.

б) В одиннадцатеричной системе счисления представление A в виде $11a+b$ дает, что при делении на 7 число A равноделимо с $a+2b$.

в) В двенадцатеричной системе счисления, представляя A в виде $12a+b$, получаем, что при делении на 17 число A равноделимо с $a-7b$.

53. Условия а) и б) выполняются автоматически. Условия в) и г) соблюдаются потому, что переход от A к $F_m(A)$ сводится к замене некоторых чисел на их остатки при делении на A (которые меньше самих чисел и равноостаточны с ними).

54. а) $r_2 = r_3 = \ldots = r_n = 0$, т. е. $r_k = 0$ $(k \geqq 2)$;
б) $r_3 = r_4 = \ldots = r_n = 0$, т. е. $r_k = 0$ $(k \geqq 3)$;
в) $r_1 = r_2 = \ldots = r_n = 1$, т. е. $r_k = 1$;
г) $r_1 = r_3 = \ldots = r_{2t-1} = -1$, $r_2 = r_4 = \ldots = r_{2t} = 1$, т. е. $r_k = (-1)^k$;
д) $r_{6t+1} = 3$, $r_{6t+2} = 2$, $r_{6t+3} = 6$, $r_{6t+4} = 4$, $r_{6t+5} = 5$, $r_{6t} = 1$.

55. Предоставляется читателю.

56. Возьмем произвольное m и положим

r_1 равным остатку от деления t на m,

r_2 равным остатку от деления tr_1 на m

и т. д. Тогда число

$$a_n t^n + a_{n-1} t^{n-1} + \ldots + a_1 t + a_0$$

оказывается при делении на m равноостаточным с числом

$$a_n r_n + a_{n-1} r_{n-1} + \ldots + a_1 r_1 + a_0.$$

После этого построение требуемого признака не составляет труда.

57. Предоставляется читателю.

58. $10^2 = 7 \cdot 14 + 2$, так что $r = 2$, и мы имеем

$$A_0 = 1\,048\,576, \quad A_1 = 1 \cdot 2^3 + 4 \cdot 2^2 + 85 \cdot 2 + 76 = 270,$$
$$A_2 = 2 \cdot 2 + 70 = 74, \quad A_3 = 4.$$

59. Если t равноостаточно с $r = r_1$ при делении на m, то

tr_1 равноостаточно с $r^2 = r_2$ при делении на m,

tr_2 равноостаточно с $r^3 = r_3$ при делении на m,

и т. д.

60. Ни $2^4 - 2$, ни $2^3 - 1$ не делятся на 4.

61. Если $a \vdots p$, то $a^p \vdots p$, и теорема доказана. Если же a не делится на p, то a взаимно просто с p, и мы можем приведенное в условии теоремы сравнение сократить:

$$a^{p-1} \equiv 1 \pmod{p}.$$

Для доказательства последнего сравнения разделим каждое из чисел вида ta $(t = 1, 2, \ldots, p-1)$ на p с остатком:

$$ta = q_t p + r_t.$$

Это можно переписать так:

$$\begin{aligned} a &\equiv r_1 \pmod p, \\ 2a &\equiv r_2 \pmod p, \\ &\cdots\cdots\cdots\cdots \\ (p-1)a &\equiv r_{p-1} \pmod p. \end{aligned} \qquad \text{(Р.11)}$$

Из результата задачи 26 следует, что среди чисел r_i ровно по одному разу встретится каждое из чисел 1, 2, ..., $p-1$. Перемножая все сравнения, мы получаем

$$1 \cdot 2 \ldots (p-1)a^{p-1} \equiv 1 \cdot 2 \ldots (p-1) \pmod p.$$

Нам остается сократить это сравнение на $1 \cdot 2 \cdot \ldots \cdot (p-1)$.

62. $\varphi(12) = \varphi(2^2 \cdot 3) = 2^{2-1}(3-1) = 2 \cdot 2 = 4,$

$$\varphi(120) = \varphi(2^3 \cdot 3 \cdot 5) = 2^{3-1}(3-1)(5-1) = 4 \cdot 2 \cdot 4 = 32,$$

$$\varphi(1000) = \varphi(2^3 \cdot 5^3) = 2^{3-1}5^{3-1}(5-1) = 4 \cdot 25 \cdot 4 = 400.$$

63. Будем искать m в виде $p_1^{\alpha_1}p_2^{\alpha_2} \ldots p_k^{\alpha_k}$. Тогда

а) $p_1^{\alpha_1-1}(p_1-1)p_2^{\alpha_2-1}(p_2-1)\ldots p_k^{\alpha_k-1}(p_k-1)=10.$

Стоящее слева произведение должно делиться на 5. Значит, либо одно из чисел $p_1, p_2, \ldots, p_k$ есть 5 (пусть для определенности $p_1 = 5$), либо на 5 делится одна из разностей $p_1 - 1, p_2 - 1, \ldots, p_k - 1$ (пусть в этом случае $(p_1 - 1) \vdots 5$). В первом из этих случаев $p_1 - 1 = 4$, чего не может быть, так как 10 на 4 не делится. Второй случай, поскольку p_1 должно быть простым числом и $10 \vdots (p_1 - 1)$, возможен лишь при $p_1 = 11$. Но тогда $\alpha_1 = 1$, и из теоремы 25 следует, что

$$\varphi\left(\frac{m}{11}\right) = 1,$$

т. е. либо $\frac{m}{11} = 1$, либо $\frac{m}{11} = 2$.

В итоге мы имеем $m_1 = 11$, $m_2 = 22$.

б) $p_1^{\alpha_1-1}(p_1-1)p_2^{\alpha_2-1}(p_2-1)\ldots p_k^{\alpha_k-1}(p_k-1)=8.$

Если m нечетное, то $\alpha_1 = \alpha_2 = \ldots = \alpha_k = 1$ (ибо правая часть написанного равенства есть степень двойки):

$$(p_1-1)(p_2-1)\ldots(p_k-1)=8.$$

Это возможно лишь при $k=2$, $p_1=3$, $p_2=5$, т. е. при $m=15$.

Пусть теперь число m четное. Положим для определенности $p_1=2$. Очевидно, по-прежнему $\alpha_2=\ldots$ $\ldots=\alpha_k=1$, и мы имеем

$$2^{\alpha-1}(p_2-1)\ldots(p_k-1)=8.$$

Очевидно, $\alpha\leqq 4$. Если $\alpha=1$, то случай подобен рассмотренному: написанное неравенство возможно также лишь при $k=3$, $p_2=3$, $p_3=5$, т. е. при $m=30$.

Если $\alpha=2$, то $k=2$, $p_2=5$ и $m=20$.

Если $\alpha=3$, то $k=2$, $p_2=3$ и $m=24$.

Если, наконец, $\alpha=4$, то $k=1$ и $m=16$.

Итак, решения нашей задачи: $m_1=15$, $m_2=30$, $m_3=20$, $m_4=24$, $m_5=16$.

64. Предположим, что

$$p_1^{\alpha_1-1}(p_1-1)\,p_2^{\alpha_2-1}(p_2-1)\ldots p_k^{\alpha_k-1}(p_k-1)=14.$$

Каждое из чисел вида p_i-1 есть либо единица, либо четное число, и потому не может быть семеркой. Будучи на единицу меньше простого числа, оно не может равняться 14. Значит, семеркой является одно из чисел $p_i^{\alpha_i-1}$. Но тогда $p_i-1=6$, а 14 на 6 не делится.

65. Пусть $m=p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_k^{\alpha_k}$. Рассмотрим сначала случай, когда m есть степень простого числа: $m=p^{\alpha}$. Для того чтобы некоторое число было взаимно простым с m, необходимо и достаточно, чтобы оно не делилось на p. Но среди чисел 0, 1, 2, ..., $m-1$ имеется всего $\frac{m}{p}$ делящихся на p чисел. Следовательно, взаимно простых с p чисел в этом списке имеется столько:

$$m-\frac{m}{p}=m\left(1-\frac{1}{p}\right)=p^{\alpha}\left(1-\frac{1}{p}\right)=p^{\alpha-1}(p-1)=\varphi(m).$$

Заметим теперь, что для взаимной простоты a и m необходимо и достаточно, чтобы с a был взаимно прост остаток от деления a на m.

По только что установленному число остатков от деления на $p_i^{\alpha_i}$, взаимно простых с $p_i^{\alpha_i}$, равно $\varphi\left(p_i^{\alpha_i}\right)$. Но, как было выяснено в процессе решения задачи 28, из равноостаточности чисел при делении на все $p_i^{\alpha_i}$

следует их равноостаточность при делении на m, и наоборот. Кроме того, для взаимной простоты некоторого числа с m необходимо и достаточно, чтобы оно было взаимно просто с каждым из чисел $p_i^{\alpha_i}$.

Следовательно, каждой комбинации остатков от деления на $p_1^{\alpha_1}$, $p_2^{\alpha_2}$, ..., $p_k^{\alpha_k}$, взаимно простых с соответствующими делителями, соответствует ровно один остаток от деления на m, взаимно простой с m. Нам остается заметить, что число таких комбинаций остатков равно

$$\varphi\left(p_1^{\alpha_1}\right)\varphi\left(p_2^{\alpha_2}\right)\ldots\varphi\left(p_k^{\alpha_k}\right)=\varphi(m).$$

66. Мы имеем

$$a_1=A+q_1m_1,\quad a_2=A+q_2m_2.$$

Поэтому

$$(a_1m_2+a_2m_1)(m_1+m_2)^{\varphi(m_1m_2)-1}=$$

$$=(A(m_1+m_2)+(q_1+q_2)m_1m_2)(m_1+m_2)^{\varphi(m_1m_2)-1}=$$

$$=A(m_1+m_2)^{\varphi(m_1m_2)}+(q_1+q_2)m_1m_2(m_1+m_2)^{\varphi(m_1m_2)-1}.$$

Здесь по теореме Эйлера первое слагаемое при делении на m_1m_2 равноостаточно с A, а второе делится на m_1m_2. Значит, вся сумма при делении на m_1m_2 равноостаточна с A.

67. Предоставляется читателю.

68. Предоставляется читателю.

69. Предоставляется читателю.

70. $n^{13}-n=n(n^{12}-1)$. Но

$$n^{12}=n^{\varphi(13)}=n^{2\varphi(7)}=n^{3\varphi(5)}=n^{6\varphi(3)}=n^{12\varphi(2)}.$$

Поэтому либо $n\vdots p$, либо $(n^{12}-1)\vdots p$ для $p=2$, 3, 5, 7, 13. Остается сослаться на теорему 16.

71. Предоставляется читателю.

72. Предоставляется читателю.

73. Пусть наибольший общий делитель чисел a и b есть d. Если c не делится на d, то уравнение

$$ax+by=c$$

в целых числах неразрешимо. Если же c делится на d, то обе части уравнения можно сократить на d, и мы приходим к уже рассмотренному случаю.

74. Пусть A и B таковы, что

$$aA+bB=1.$$

Положим

$$x_t = cA + bt,$$

$$y_t = c\frac{1-aA}{b} - at.$$

Тогда

$$ax_t + by_t = a(cA + bt) + b\left(c\frac{1-aA}{b} - at\right) =$$

$$= caA + abt + c(1 - aA) - abt = c,$$

и (x_t, y_t) действительно является решением нашего уравнения.

75. а) $x_t = 9 \cdot 5^5 + 7t = 28\,125 + 7t,$

$$y_t = 9\frac{1-5^6}{7} - 5t = -20\,088 - 5t.$$

Поскольку свободные члены и коэффициенты при t в выражениях для x_t и y_t, так сказать, «примерно пропорциональны», мы можем надеяться получить представления наших решений в меньших числах. В самом деле, мы можем написать:

$$x_t = 6 + 7(t + 4017),$$

$$y_t = -3 - 5(t + 4017),$$

или, полагая

$$t + 4017 = t',$$

получаем

$$x_{t'} = 6 + 7t',$$

$$y_{t'} = -3 - 5t'.$$

Заметим, что способ решения уравнений в целых числах, приведенный в задаче 74, позволяет обходиться меньшими числами, хотя и требует несколько более сложных вычислений.

б) Воспользуемся тем, что 25 по модулю 13 принадлежит показателю 2. Мы можем написать:

$$x_t = 8 \cdot 25 + 13t = 200 + 13t,$$

$$y_t = 8\frac{1-25^2}{13} - 25t = -384 - 25t,$$

или после упрощений

$$x_{t'} = 5 + 13t',$$

$$y_{t'} = -9 - 25t'.$$

76. Условие в) обеспечивается автоматически, а условие г) следует из теоремы 25.

77.

m	17	19	27	29	31	49
k'	12 (или -5)	2	19	3	28 (или -3)	5

78. Предоставляется читателю.

79. Предоставляется читателю.

80. а) $8^{\varphi(21)-1} = 8^{11} = 64^5 \cdot 8$. При делении на 21 это число равноостаточно с 8. Значит, числа $8a + b$ и $a + 8b$ равноделимы на 21.

б) $12^{\varphi(31)-1} = 12^{29} = (12^2)^{14} \cdot 12 = 144^{14} \cdot 12$ при делении на 31 равноостаточно с $11^{14} \cdot 12 = 121^7 \cdot 12 = (-3)^7 \cdot 12 = -(3^3)^2 \cdot 3 \cdot 12 = -(31-4)^2(31+5)$, что равноостаточно с $-16 \cdot 5 = -80$. Последнее число очевидно равноостаточно с 13. Значит, числа $12a + b$ и и $a + 13b$ равноделимы на 31.

СОДЕРЖАНИЕ

Предисловие 3
§ 1. Делимость чисел 7
§ 2. Делимость сумм и произведений 24
§ 3. Признаки равноостаточности и признаки делимости . . 30
§ 4. Общие признаки равноостаточности и делимости . . . 47
§ 5. Делимость степеней 52
Доказательства теорем 60
Решения задач 71

Николай Николаевич Воробьев

ПРИЗНАКИ ДЕЛИМОСТИ

Серия «Популярные лекции
по математике», выпуск 39

Редактор *В. В. Донченко*

Художественный редактор *Т. Н. Кольченко*

Технический редактор *И. Ш. Аксельрод*

Корректоры *Л. И. Назарова, Т. С. Вайсберг*

ИБ № 32618

Сдано в набор 15.05.87. Подписано к печати 14.10.87. Формат 84×108/32. Бумага тип. № 2. Гарнитура литературная. Печать высокая. Усл. печ. л. 5,04. Усл. кр.-отт. 5,25. Уч.-изд. л. 4,98. Тираж 165 000 экз. Заказ № 589. Цена 20 коп.

Ордена Трудового Красного Знамени
издательство «Наука»
Главная редакция
физико-математической литературы
117071 Москва В-71, Ленинский проспект, 15

Ленинградская типография № 2 головное предприятие ордена Трудового Красного Знамени Ленинградского объединения «Техническая книга» имени Евгении Соколовой Союзполиграфпрома при Государственном комитете СССР по делам издательств, полиграфии и книжной торговли. 198052, г. Ленинград, Л-52, Измайловский проспект, 29

ПОПУЛЯРНЫЕ ЛЕКЦИИ ПО МАТЕМАТИКЕ

Вып. 1. **А. И. Маркушевич.** Возвратные последовательности.
Вып. 2. **И. П. Натансон.** Простейшие задачи на максимум и минимум.
Вып. 3. **И. С. Соминский.** Метод математической индукции.
Вып. 4. **А. И. Маркушевич.** Замечательные кривые.
Вып. 5. **П. П. Коровкин.** Неравенства.
Вып. 6. **Н. Н. Воробьев.** Числа Фибоначчи.
Вып. 7. **А. Г. Курош.** Алгебраические уравнения произвольных степеней.
Вып. 8. **А. О. Гельфонд.** Решение уравнений в целых числах.
Вып. 9. **А. И. Маркушевич.** Площади и логарифмы.
Вып. 10. **А. С. Смогоржевский.** Метод координат.
Вып. 11. **Я. С. Дубнов.** Ошибки в геометрических доказательствах.
Вып. 12. **И. П. Натансон.** Суммирование бесконечно малых величин.
Вып. 13. **А. И. Маркушевич.** Комплексные числа и конформные отображения.
Вып. 14. **А. И. Фетисов.** О доказательствах в геометрии.
Вып. 15. **И. Р. Шафаревич.** О решении уравнений высших степеней.
Вып. 16. **В. Г. Шерватов.** Гиперболические функции.
Вып. 17. **В. Г. Болтянский.** Что такое дифференцирование?
Вып. 18. **Г. М. Миракьян.** Прямой круговой цилиндр.
Вып. 19. **Л. А. Люстерник.** Кратчайшие линии.
Вып. 20. **А. М. Лопшиц.** Вычисление площадей ориентированных фигур.
Вып. 21. **Л. И. Головина** и **И. М. Яглом.** Индукция в геометрии.
Вып. 22. **В. Г. Болтянский.** Равновеликие и равносоставленные фигуры.
Вып. 23. **А. С. Смогоржевский.** О геометрии Лобачевского.
Вып. 24. **Б. И. Аргунов** и **Л. А. Скорняков.** Конфигурационные теоремы.
Вып. 25. **А. С. Смогоржевский.** Линейка в геометрических построениях.
Вып. 26. **Б. А. Трахтенброт.** Алгоритмы и машинное решение задач.
Вып. 27. **В. А. Успенский.** Некоторые приложения механики к математике.
Вып. 28. **Н. А. Архангельский** и **Б. И. Зайцев.** Автоматические цифровые машины.
Вып. 29. **А. Н. Костовский.** Геометрические построения одним циркулем.
Вып. 30. **Г. Е. Шилов.** Как строить графики.

Вып. 31. **А. Г. Дорфман.** Оптика конических сечений.
Вып. 32. **Е. С. Вентцель.** Элементы теории игр.
Вып. 33. **А. С. Барсов.** Что такое линейное программирование.
Вып. 34. **Б. Е. Маргулис.** Системы линейных уравнений.
Вып. 35. **Н. Я. Виленкин.** Метод последовательных приближений.
Вып. 36. **В. Г. Болтянский.** Огибающая.
Вып. 37. **Г. Е. Шилов.** Простая гамма (устройство музыкальной шкалы).
Вып. 38. **Ю. А. Шрейдер.** Что такое расстояние?
Вып. 39. **Н. Н. Воробьев.** Признаки делимости.
Вып. 40. **С. В. Фомин.** Системы счисления.
Вып. 41. **Б. Ю. Коган.** Приложение механики к геометрии.
Вып. 42. **Ю. И. Любич и Л. А. Шор.** Кинематический метод в геометрических задачах.
Вып. 43. **В. А. Успенский.** Треугольник Паскаля.
Вып. 44. **И. Я. Бакельман.** Инверсия.
Вып. 45. **И. М. Яглом.** Необыкновенная алгебра.
Вып. 46. **И. М. Соболь.** Метод Монте-Карло.
Вып. 47. **Л. А. Калужнин.** Основная теорема арифметики.
Вып. 48. **А. С. Солодовников.** Системы линейных неравенств.
Вып. 49. **Г. Е. Шилов.** Математический анализ в области рациональных функций.
Вып. 50. **В. Г. Болтянский, И. Ц. Гохберг.** Разбиение фигур на меньшие части.
Вып. 51. **Н. М. Бескин.** Изображения пространственных фигур.
Вып. 52. **Н. М. Бескин.** Деление отрезка в данном отношении.
Вып. 53. **Б. А. Розенфельд и Н. Д. Сергеева.** Стереографическая проекция.
Вып. 54. **В. А. Успенский.** Машина Поста.
Вып. 55. **Л. Беран.** Упорядоченные множества.
Вып. 56. **С. А. Абрамов.** Элементы программирования.
Вып. 57. **В. А. Успенский.** Теорема Геделя о неполноте.
Вып. 58. **Ю. А. Шашкин.** Эйлерова характеристика.
Вып. 59. **Л. А. Скорняков.** Системы линейных уравнений.

20 коп.